SoftControl

Service Center 4.2.505

Руководство администратора

Уважаемый пользователь!

SAFE ‘N SEC Corporation благодарит Вас за то, что выбрали продукт SoftControl Service Center. Специалисты компании постарались, чтобы наше программное обеспечение отвечало самым высоким требованиям в области защиты информации и в то же время было простым и удобным в работе. Мы надеемся, что SoftControl Service Center будет Вам полезен.

Почтовый адрес:
127106, Россия, Москва
Алтуфьевское шоссе, 5/2
SAFE ‘N SEC Corporation
Телефон:
+7 (495) 967-14-51
Факс:
+ 7 (495) 967-14-52
Электронная почта:
Общие вопросы и предложения: support@safensoft.com
Коммерческие вопросы: sales@safensoft.com
Веб-сайт компании: http://www.safensoft.com

Содержание

1. Введение 5
1.1 Назначение 5
1.2 Условные обозначения и термины 5
1.2.1 Обозначения 5
1.2.2 Сокращения 6
1.2.3 Глоссарий 6
2. Требования к аппаратному и программному обеспечению 8
2.1 Системные требования SoftControl Server 8
2.2 Системные требования SoftControl Admin Console 8
3. Установка и настройка компонентов SoftControl Service Center 9
3.1 Установка SoftControl Server и SoftControl Admin Console 9
3.1.1 Обычная установка 9
3.1.2 Полная установка 12
3.1.3 Выборочная установка 16
3.2 Настройка сервера 19
3.3 Регистрация клиентских приложений 24
3.4 Подключение к серверу из консоли управления 24
4. Централизованное управление СИБ 26
4.1 Интерфейс SoftControl Admin Console 26
4.2 Порядок работы 29
4.3 Управление доступом на основе ролей 30
4.3.1 Роли 30
4.3.2 Пользователи 33
4.3.3 События безопасности сервера 35
4.4 Устройства и статусы 39
4.4.1 Управление процессом регистрации 43
4.4.2 Перемещение в подразделения 45
4.4.3 Управление списком разрешённых файлов 45
4.5 Подразделения 46
4.5.1 Управление подразделениями 48
4.5.2 Генерация одноразовых паролей 50
4.6 Настройка клиентских приложений 52
4.6.1 Общие настройки 55
4.6.2 Настройки SoftControl SysWatch 59
4.6.3 Настройки SoftControl DLP Client 88
4.7 Задачи 98

4.7.1 Сбор профиля 101
4.7.2 Антивирусное сканирование 102
4.7.3 Обновление 104
4.8 Просмотр отчётов 106
4.8.1 Отчёты SoftControl SysWatch 106
4.8.2 Отчёты SoftControl DLP Client 113
4.8.3 Фильтрация событий 118
4.8.4 Печать и экспорт в файлы отчётов 123
4.9 Оповещения о событиях 124
4.9.1 Контакты 125
4.9.2 Нотификации 126
5. Обновление компонентов СИБ 132
5.1 Настройка обновления программных модулей 132
5.2 Настройка обновления антивирусных баз 135
5.3 Обновление SoftControl Server и SoftControl Admin Console в ручном режиме 138
5.4 Обновление клиентских компонентов 141
6. Удаление компонентов SoftControl Service Center 143
7. Дополнительная информация 147
7.1 О сертификатах сервера 147
7.2 Восстановление связи с сервером 148
7.3 Резервное копирование SoftControl Service Center 149
7.3.1 Создание резервной копии 149
7.3.2 Восстановление из резервной копии 150
7.4 Источники 151
8. Диагностика проблем 153
9. Техническая поддержка 154
10. Приложение 155
10.1 Установка и настройка Microsoft® SQL Server® 2008 155
10.2 Добавление компонента Desktop Experience 171

1. Введение

1.1 Назначение

SoftControl Service Center («Сервисный Центр») представляет собой набор инструментов администрирования для управления системой информационной безопасности, обеспечивающей сохранение целостности программной среды конечных точек сети, защиту от несанкционированного доступа к данным со стороны персонала или злоумышленников, а также мониторинг активности пользователей. В состав Сервисного Центра входят следующие компоненты:

- SoftControl Server – серверный компонент;
- SoftControl Admin Console – консоль управления.

SoftControl Service Center поддерживает работу со следующими клиентскими компонентами:

- SoftControl ATM Client / Endpoint Client / SClient (далее по тексту – SoftControl SysWatch) – клиентские компоненты проактивной защиты устройств самообслуживания, рабочих станций корпоративной сети и серверов соответственно;
- SoftControl DLP Client – клиентский компонент мониторинга и сбора данных.

1.2 Условные обозначения и термины

1.2.1 Обозначения

Условные обозначения, применяемые в данном документе, приведены в табл. 1.

Таблица 1. Условные обозначения

Пример обозначения	Описание
	Важная информация, примечание.
Условие	Условие выполнения, примечание, пример.
Обновить	– заголовки и сокращения; – названия экранных кнопок, ссылок, пунктов меню, других элементов программного интерфейса.
Политика контроля	– термины (определения); – имена файлов и других объектов; – тексты сообщений, выводимых пользователю.
`C:\Program Files\SoftControl`	Пути к файлам, каталогам, ключам системного реестра.
`%windir%\system32\msiexec.exe /i`	Фрагменты программного кода, командных и конфигурационных файлов.
<каталог установки SoftControl	Поля для замены функциональных названий фактическими

Пример обозначения	Описание
SysWatch>	значениями.
Приложение 5	Ссылки на внутренние ресурсы (разделы документа) с указанием номера страницы или на внешние ресурсы (URL-адреса).

1.2.2 Сокращения

В данном документе употребляются без расшифровки следующие сокращения:

- **БД** – база данных;
- **ГИП** – графический интерфейс пользователя;
- **ЛВС** – локальная вычислительная сеть;
- **ОЗУ** – оперативное запоминающее устройство;
- **ОС** – операционная система;
- **ПО** – программное обеспечение;
- **СИБ** – система информационной безопасности;
- **СУБД** – система управления базами данных;
- **ЦП** – центральный процессор;
- **ЭЦП** – электронная цифровая подпись.

1.2.3 Глоссарий

Таблица 2. Глоссарий

Термин	Пояснение
Проактивная защита	Комплекс мер по предотвращению вредоносных воздействий, основанный на превентивных технологиях.
Превентивные технологии	Передовые технологии защиты данных, в основе которых лежит анализ активности на компьютере пользователя: действий любых приложений, служб операционной системы, действий пользователя, активности извне и т.д. В отличие от реактивных технологий, на которых построены такие средства защиты как антивирусы и персональные сетевые экраны, превентивные технологии анализируют не код объекта, а отслеживают потенциально опасные действия, выполняемые им. Следовательно, инструменты проактивной защиты не требуют наличия и постоянного обновления баз вредоносного кода, что является необходимым для традиционных средств защиты.
Политика контроля	Набор правил, на основании которых осуществляется контроль активности приложений и их анализ, а также выносится заключение об опасности приложения. Именно политика определяет, какие действия и какую их

Термин	Пояснение
	последовательность считать опасной.
Правило контроля активности	Набор условий, определяющих активность приложения, и действия, которые применяет средство проактивной защиты к приложению с активностью, удовлетворяющей условиям правила. Условия правила определяют область контроля и детализируют ее (объект контроля, действие над объектом контроля, приложение, выполняющее действие и т.д.).
Профиль системы	Совокупность контрольных сумм переносимых исполняемых модулей (см. "файловый формат PE") и путей к ним в системе, полученная в результате автоматической настройки (сбора профиля).
Признак инсталлятора	Специальный флаг, дающий процессу особые привилегии по запуску (см. "режим установки").
Режим установки	Режим запуска процессов без ограничений, при котором происходит помещение процесса и всех его дочерних процессов в профиль системы, если он еще не находится там.
Реактивные (сигнатурные) технологии	Метод работы антивирусного программного обеспечения и систем обнаружения вторжений, при котором программа в процессе анализа объекта обращается к базе данных известных вирусов и проверяет соответствие какого-либо участка кода просматриваемого объекта известному коду (сигнатуре) вируса в базе данных.
Роль	Совокупность прав доступа на объекты компьютерной системы.
Файловый формат PE (переносимый исполняемый файл)	Формат исполняемых файлов, объектного кода и динамических библиотек, используемый в 32- и 64-битных версиях операционной системы Microsoft® Windows®.
Хост	Средство вычислительной техники (рабочая станция / сервер / терминал самообслуживания), подключенное к локальной вычислительной сети или глобальной компьютерной сети.

2. Требования к аппаратному и программному обеспечению

2.1 Системные требования SoftControl Server

Таблица 3. Минимальные системные требования

ОС	Частота ЦП	Объём ОЗУ	Объём свободного пространства на жёстком диске
▪ Microsoft® Windows® 7 (SP1) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® 8 / 8.1 x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 (SP2) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 R2 ▪ Microsoft® Windows® Server 2012 ▪ Microsoft® Windows® Server 2012 R2 ▪ Microsoft® Windows® 10	3 ГГц	4 ГБ	100 МБ + дополнительно 4 ГБ в случае установки встроенной СУБД

Дополнительное ПО:

- Microsoft® .NET Framework 4.5;
- Microsoft® SQL Server® 2008 / SQL Server® 2012 / SQL Server® 2014 Express SP1.

2.2 Системные требования SoftControl Admin Console

Таблица 4. Минимальные системные требования

ОС	Частота ЦП	Объём ОЗУ	Объём свободного пространства на жёстком диске
▪ Microsoft® Windows® 7 (SP1) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® 8 / 8.1 x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 (SP2) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 R2 ▪ Microsoft® Windows® Server 2012 ▪ Microsoft® Windows® Server 2012 R2 ▪ Microsoft® Windows® 10	3 ГГц	4 ГБ	100 МБ

Дополнительное ПО:

- Microsoft® .NET Framework 4.5.

3. Установка и настройка компонентов SoftControl Service Center

В настоящем разделе приведена информация по установке [9] серверного компонента SoftControl Server («сервера») и консоли управления SoftControl Admin Console, настройке [19] SoftControl Server при первом запуске [24] SoftControl Admin Console, а также даны указания по регистрации клиентских приложений [24].

3.1 Установка SoftControl Server и SoftControl Admin Console

Возможны следующие варианты развёртывания SoftControl Service Center:

- обычная [9]: установка компонентов продукта без встроенной СУБД;
- полная [12]: установка компонентов продукта и встроенной СУБД;
- выборочная [16]: установка выбранных пользователем компонентов.

Если в сетевом доступе имеется настроенная СУБД или если её планируется установить отдельно, выберите вариант обычной установки. Информация по отдельной установке СУБД дана в приложении [155].

Для наиболее быстрого развёртывания и настройки выберите вариант полной установки, в этом случае все необходимые действия, включая установку входящей в инсталлятор СУБД и создание БД, выполняются установщиком SoftControl Service Center автоматически. В пакет установки SoftControl Service Center входит бесплатная СУБД Microsoft® SQL Server® 2014 Express SP1, обладающая всей необходимой функциональностью для работы сервера.

Если предпочтительно устанавливать серверный компонент, СУБД и консоль управления на разные компьютеры, используйте выборочную установку.

3.1.1 Обычная установка

1) Запустите установочный пакет *Service.Center.msi*.
2) В окне **Установка SoftControl Service Center** нажмите на кнопку **Далее** (рис. Запуск программы установки [9]).

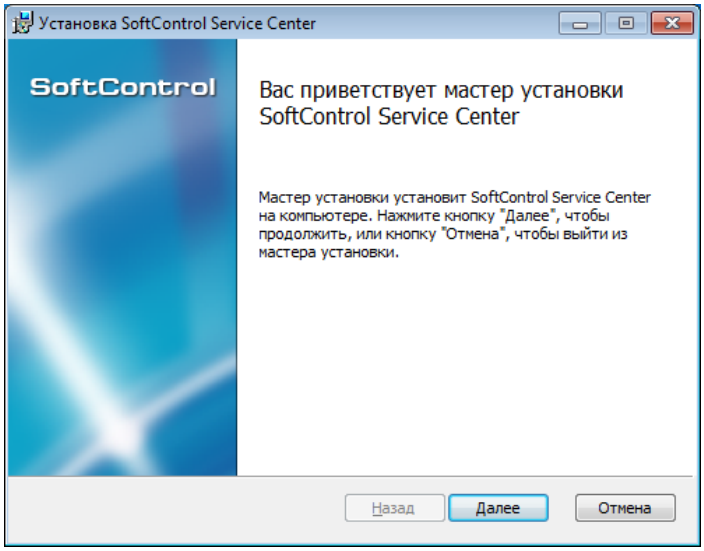


Рисунок 1. Запуск программы установки

3) В случае вашего согласия, отметьте опцию **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее** (рис. Лицензионное соглашение 10).

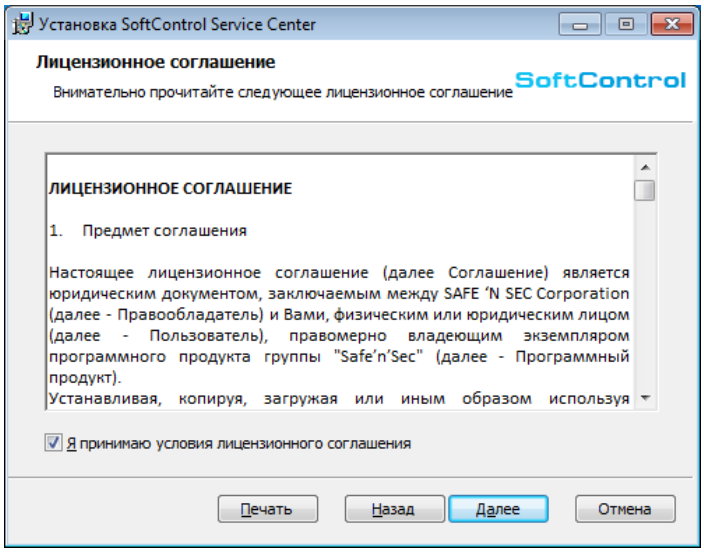


Рисунок 2. Лицензионное соглашение

4) Выберите тип установки **Обычная**, нажав на соответствующую кнопку (рис. Типы установки 10).

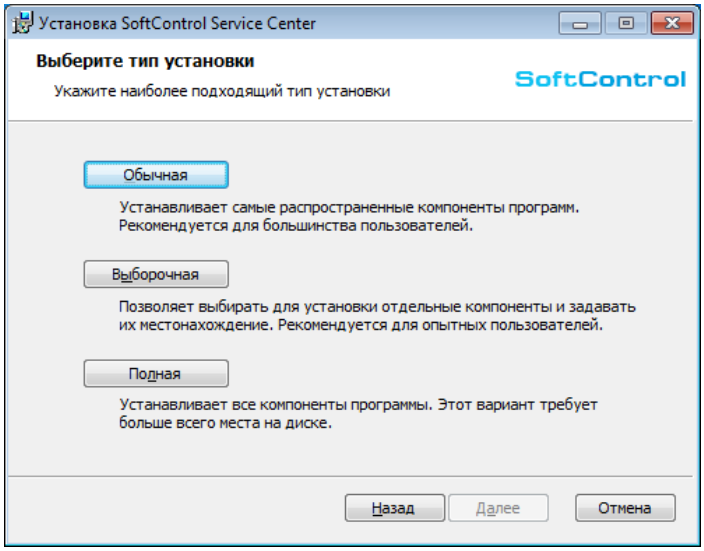


Рисунок 3. Типы установки

5) Нажмите на кнопку **Установить** (рис. Готовность к установке 11).

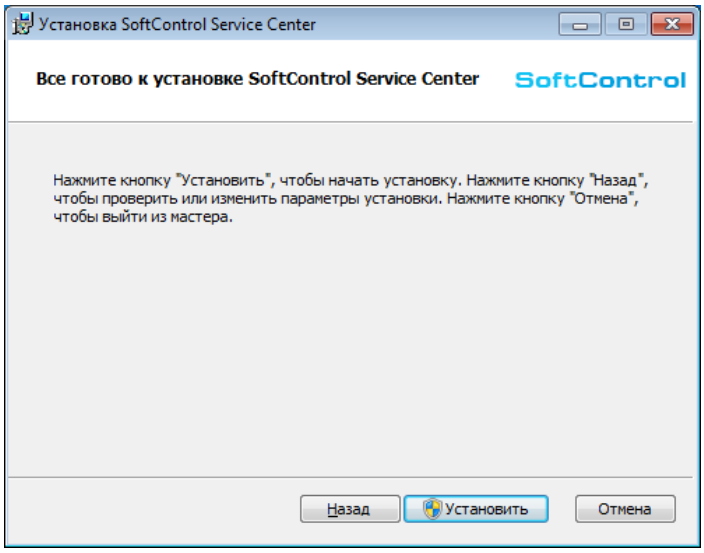


Рисунок 4. Готовность к установке

6) Дождитесь окончания процесса установки (рис. Процесс установки 11).

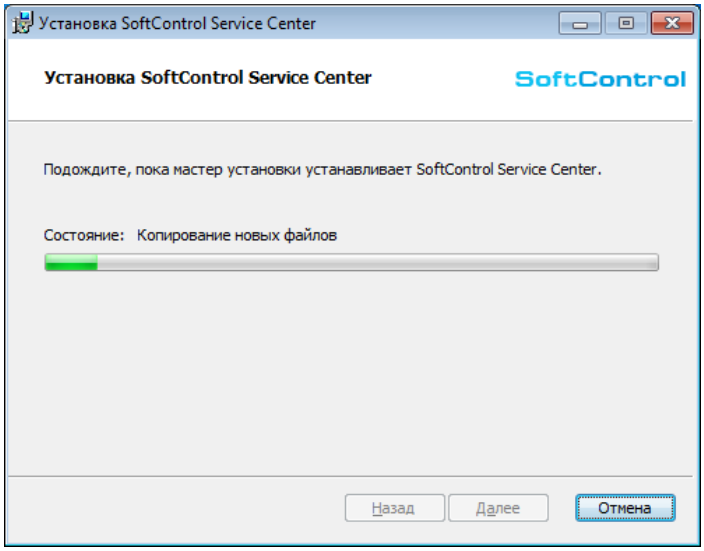


Рисунок 5. Процесс установки

7) После появления сообщения *Установка SoftControl Service Center завершена* нажмите на кнопку **Готово** (рис. Завершение установки 12).

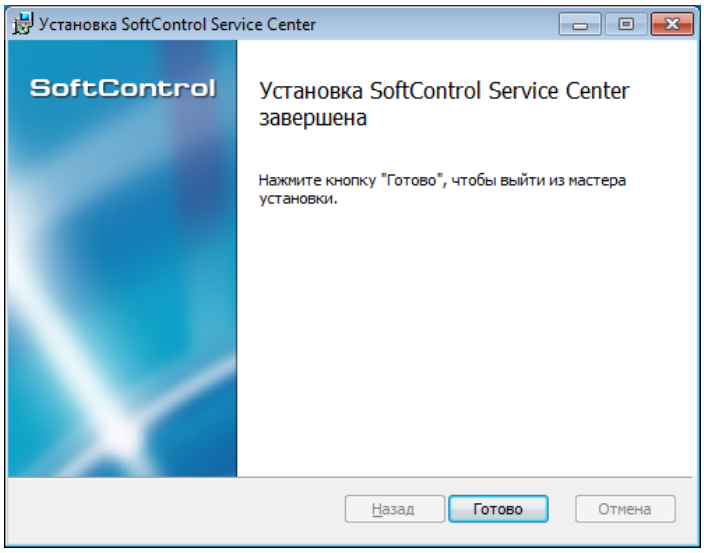


Рисунок 6. Завершение установки

3.1.2 Полная установка

1) Запустите установочный пакет *Service.Center.msi*.
2) В окне **Установка SoftControl Service Center** нажмите на кнопку **Далее** (рис. Запуск программы установки 12).

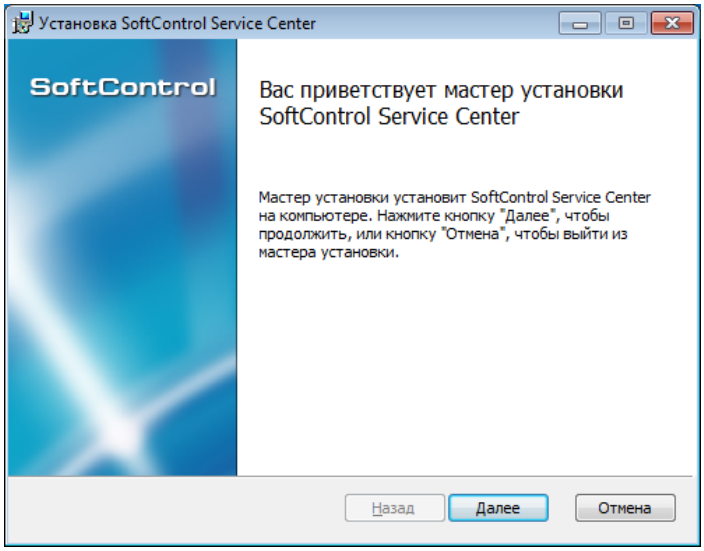


Рисунок 7. Запуск программы установки

3) В случае вашего согласия, отметьте опцию **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее** (рис. Лицензионное соглашение 13).

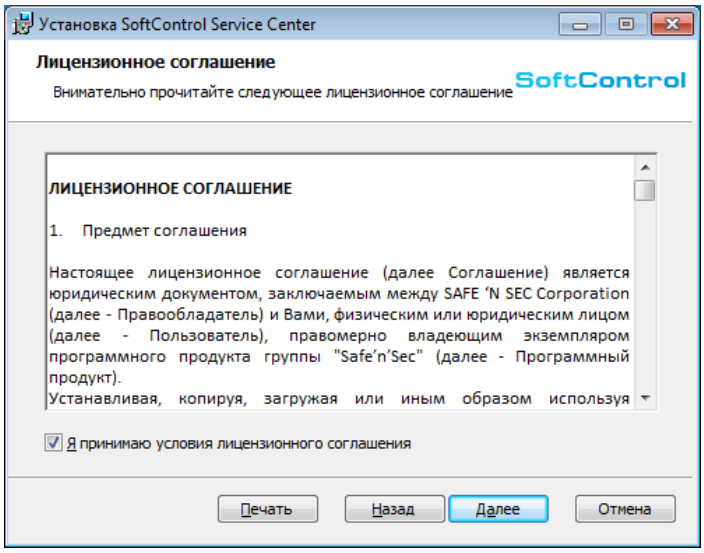


Рисунок 8. Лицензионное соглашение

4) Выберите тип установки **Полная**, нажав на соответствующую кнопку (рис. Типы установки 13).

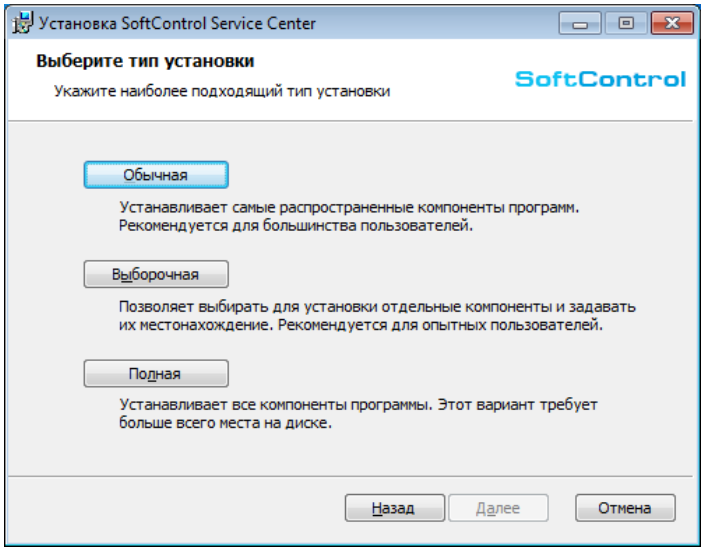


Рисунок 9. Типы установки

5) Нажмите на кнопку **Установить** (рис. Готовность к установке 14).

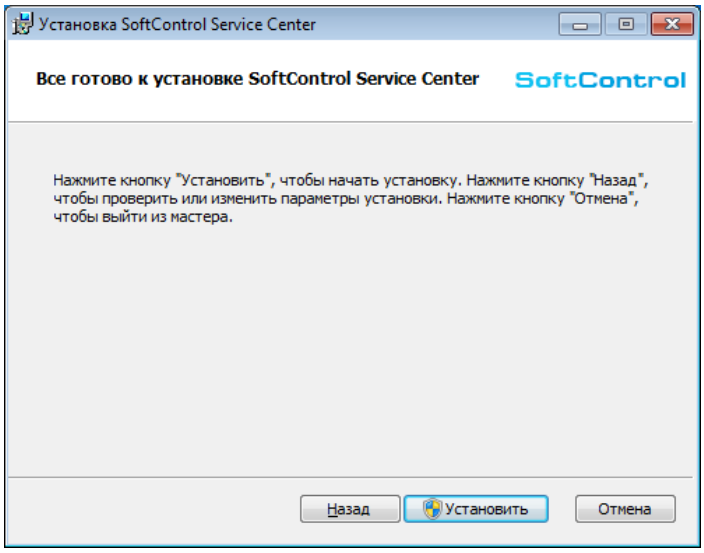


Рисунок 10. Готовность к установке

6) Дождитесь окончания процесса установки (рис. Процесс установки 14).

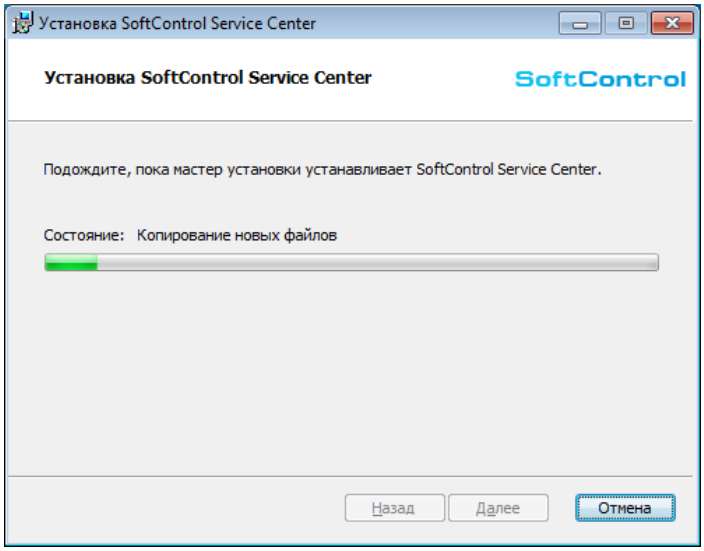


Рисунок 11. Процесс установки

7) После появления сообщения *Установка SoftControl Service Center завершена* нажмите на кнопку **Готово**, чтобы начать установку Microsoft® SQL Server® 2014 Express SP1 (рис. Завершение установки SoftControl Service Center 15).

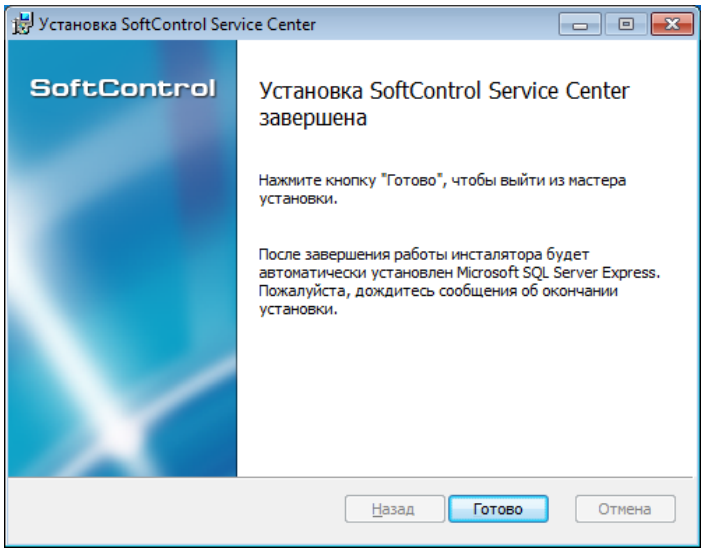


Рисунок 12. Завершение установки SoftControl Service Center

8) Дождитесь окончания установки Microsoft® SQL Server® 2014 Express SP1 и нажмите на кнопку **OK** (рис. Завершение установки 15).

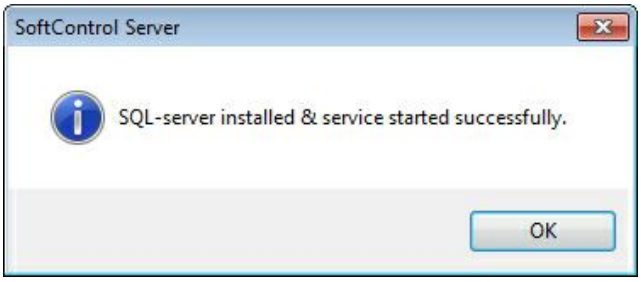


Рисунок 13. Завершение установки

3.1.3 Выборочная установка

1) Запустите установочный пакет *Service.Center.msi*.
2) В окне **Установка SoftControl Service Center** нажмите на кнопку **Далее** (рис. Запуск программы установки 16).

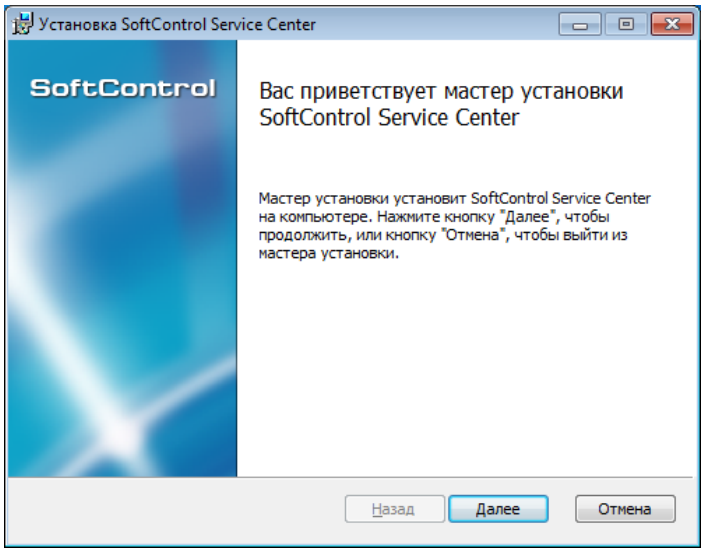


Рисунок 14. Запуск программы установки

3) В случае вашего согласия, отметьте опцию **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее** (рис. Лицензионное соглашение 16).

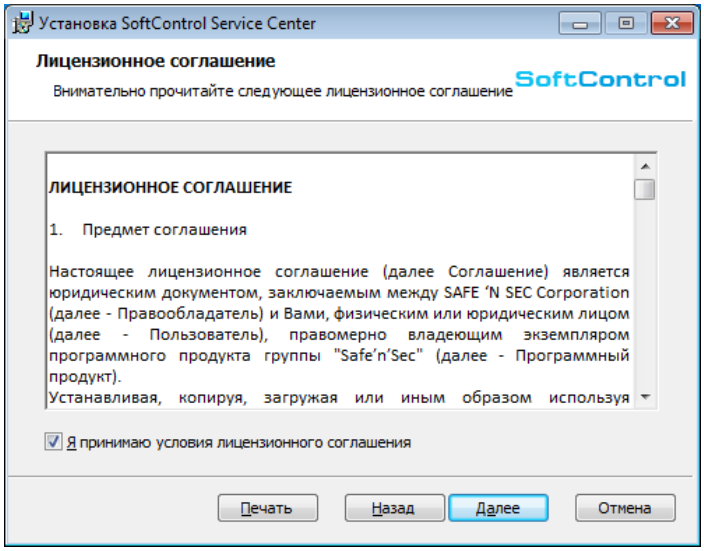


Рисунок 15. Лицензионное соглашение

4) Выберите тип установки **Выборочная**, нажав на соответствующую кнопку (рис. Типы установки 17).

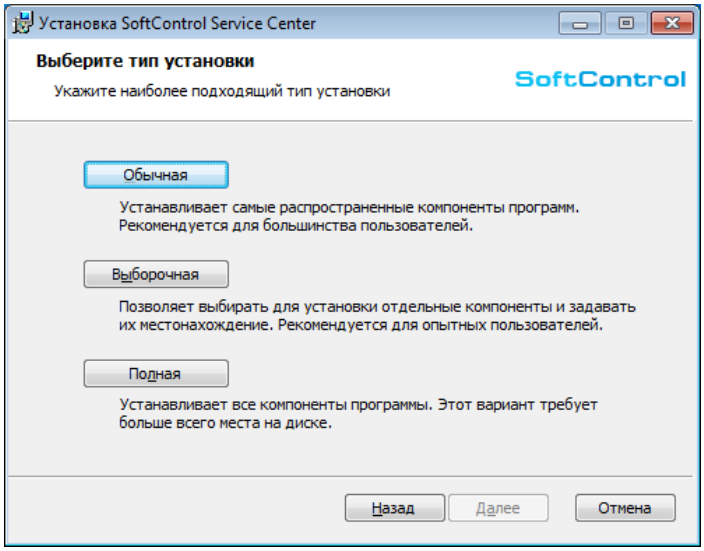


Рисунок 16. Типы установки

5) Настройте конфигурацию установки компонентов (рис. Конфигурация установки компонентов 18): нажмите на пиктограмму у компонента, который не требуется устанавливать, и в выпадающем меню выберите опцию **Компонент будет полностью недоступен** (рис. Опции установки компонента 18). Для устанавливаемого компонента должна быть выбрана опция **Будет установлен на локальный жесткий диск** (рис. Опции установки компонента 18). При необходимости измените путь установки по умолчанию, нажав на кнопку **Обзор**. С помощью кнопки **Использование диска** можно просмотреть суммарный размер устанавливаемых компонентов и доступное место на

жёстком диске. После того как все установки завершены, нажмите на кнопку **Далее**.

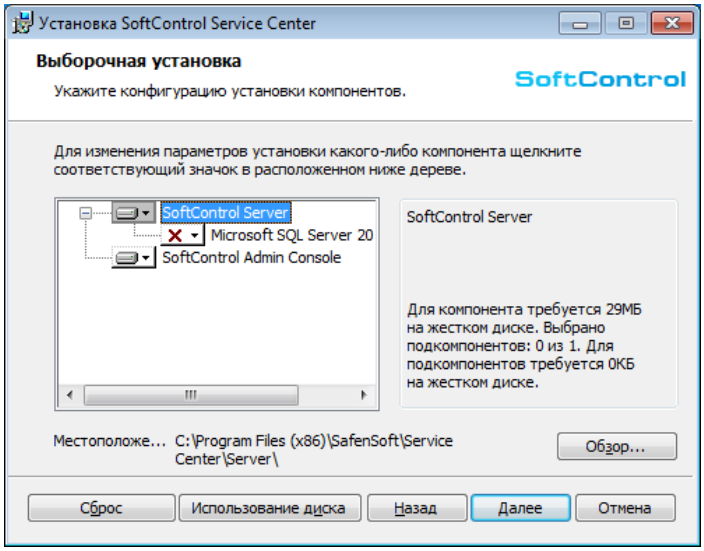


Рисунок 17. Конфигурация установки компонентов

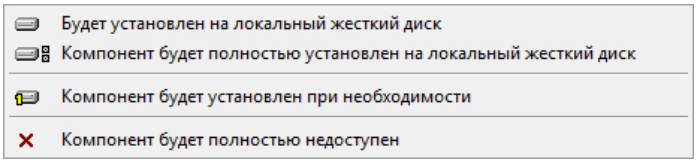


Рисунок 18. Опции установки компонента

6) Выберите опцию **Добавить необходимые порты в исключения Брандмауэра Windows** для автоматического добавления порта связи между SoftControl Admin Console и SoftControl Server в исключения брандмауэра (рис. Опция добавления порта в исключения брандмауэра 18). В обратном случае будет необходимо произвести эту операцию вручную (по умолчанию используется порт *8080*). Для продолжения установки нажмите на кнопку **Далее**.

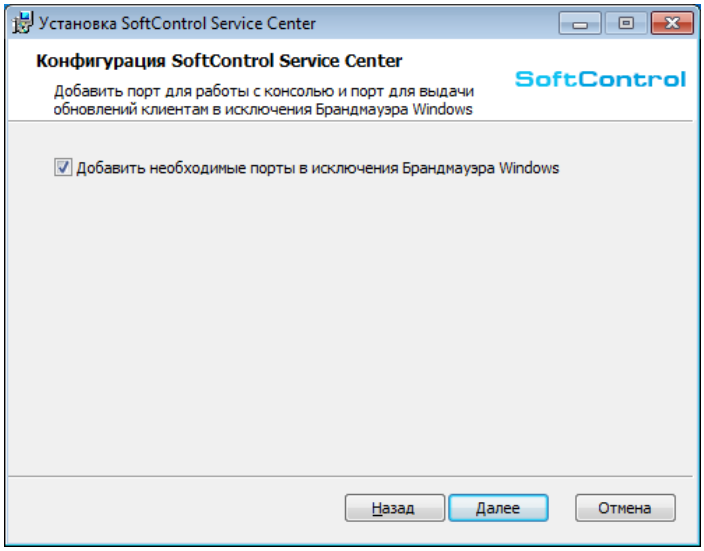


Рисунок 19. Опция добавления порта в исключения брандмауэра

7) В случае выбора установки SoftControl Admin Console *и/или* SoftControl Server без встроенной СУБД повторите действия 5-7 для обычной установки[11]. Если устанавливается SoftControl Server с подкомпонентом *Microsoft SQL Server® 2014 Express SP1*, повторите действия 5-8 для полной установки[14].

3.2 Настройка сервера

Для запуска консоли управления откройте ярлык SoftControl Admin Console на рабочем столе. В случае несконфигурированного сервера в появившемся окне введите IP-адрес компьютера с установленным SoftControl Server в поле **Адрес сервера** (допускается указывать зарезервированное имя *localhost*, если SoftControl Server и SoftControl Admin Console установлены на одном компьютере) и нажмите на кнопку **Применить** (рис. Первый запуск SoftControl Admin Console[19]).

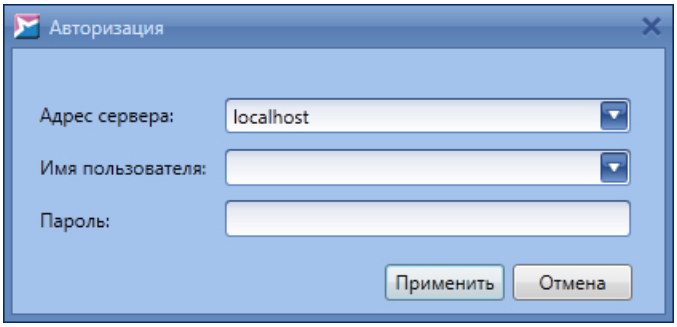


Рисунок 20. Первый запуск SoftControl Admin Console

В диалоговом окне с предложением создания первичной конфигурации сервера выберите **Да** (рис. Предложение запуска мастера настройки 20).

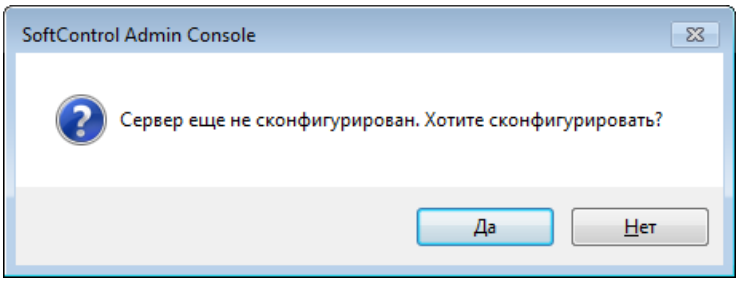


Рисунок 21. Предложение запуска мастера настройки

В окне мастера настройки сервера в разделе **База данных** задаются параметры подключения к СУБД и имя БД, которая будет использоваться серверным компонентом SoftControl Server. Поля заполняются значениями по умолчанию, если SoftControl Service Center был установлен совместно со встроенной СУБД. В других случаях или если необходимо изменить стандартные значения, введите следующие параметры (в скобках указаны значения по умолчанию) (рис. Настройка подключения к СУБД 20):

- **Сервер СУБД** – сетевой адрес (имя) сервера СУБД (*localhost\SQLTPS*);
- **Имя базы данных** – имя БД на сервере СУБД (*safensoft.tpsecure*);
- **Тип авторизации** – тип авторизации на сервере СУБД (*Авторизация SQL Server*);
- **Пользователь** – имя пользователя на сервере СУБД (*sa*);
- **Пароль** – пароль пользователя на сервере СУБД (*SafenSoft2007*).

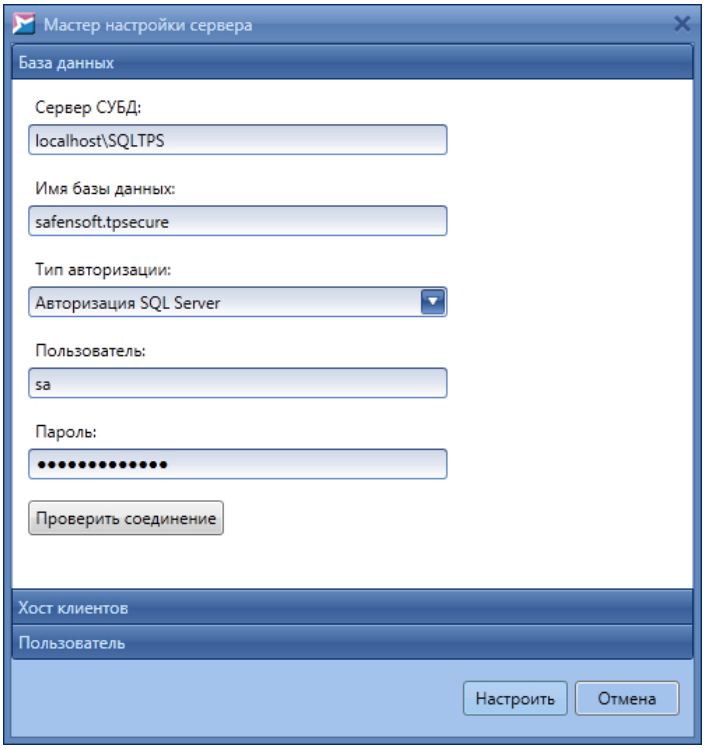


Рисунок 22. Настройка подключения к СУБД

Для проверки соединения с СУБД и корректности данных учётной записи SQL Server нажмите на кнопку **Проверить соединение**. Если БД с указанным именем не существует, то она будет создана на сервере СУБД по окончании работы мастера настройки.

В разделе **Хост клиентов** определяются параметры подключения клиентских приложений к серверу (рис. Настройка подключения клиентских приложений к серверу 21).

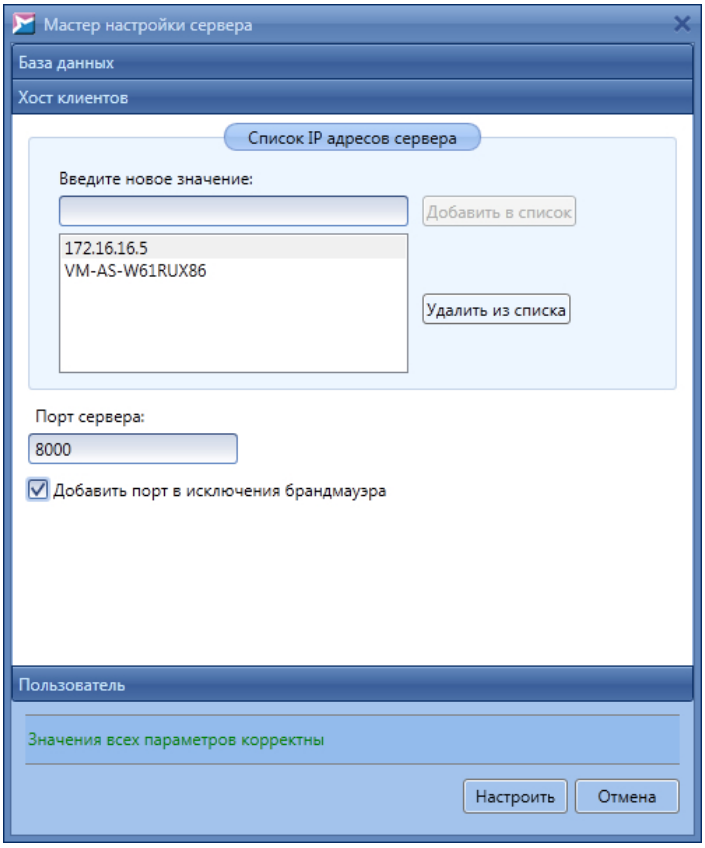


Рисунок 23. Настройка подключения клиентских приложений к серверу

По умолчанию для связи с сервером используется его текущий IP-адрес и порт *8000* протокола TCP. Возможно также осуществлять взаимодействие клиентских приложений с сервером по нескольким резервным каналам. Данная функция реализуется путём задания всех IP-адресов или NetBIOS-имён, по которым сервер доступен для клиентских приложений. В этом случае клиентский компонент осуществляет поочередное подключение по каждому из адресов до первой успешной обработки запроса, после чего связь с сервером устанавливается по данному адресу. Если подключение ни по одному из адресов неудачно, то клиентский компонент повторяет перебор адресов по истечении интервала обращения к серверу. Чтобы добавить адрес в перечень, введите новое значение в соответствующем поле и нажмите на кнопку **Добавить в список**. Чтобы удалить адрес из перечня, выберите его и нажмите на кнопку **Удалить из списка**. В поле **Порт сервера** укажите порт связи клиентских приложений с сервером (в случае установки SoftControl Server и SoftControl Admin Console на один компьютер данный порт не должен совпадать с портом связи SoftControl Server и SoftControl Admin Console [25]). Установите флажок **Добавить порт в исключения Брандмауэра Windows** в том случае, если исключение на выбранный порт отсутствует в

брандмауэре.

Настоятельно рекомендуется указывать NetBIOS-имя сервера в списке адресов, чтобы клиентские приложения не теряли связи с сервером даже в случае автоматической смены его IP-адреса. Если это все же произошло, воспользуйтесь указаниями по восстановлению связи 148.

В разделе **Пользователь** создайте учётную запись первого пользователя, введя **Имя пользователя**, **Пароль** и **Подтверждение пароля** (рис. Создание пользователя 23). Данный пользователь будет иметь права администратора.

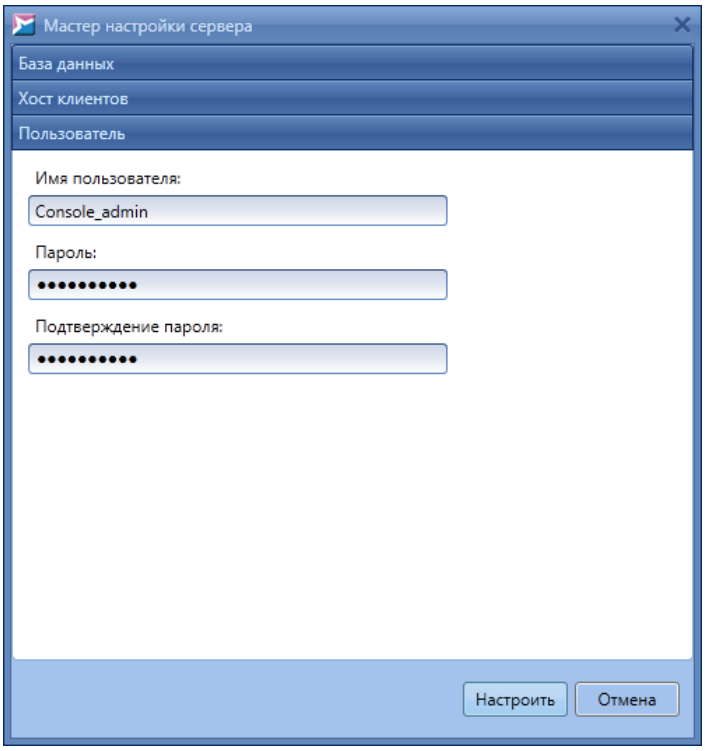


Рисунок 24. Создание пользователя

После того как все настройки введены, нажмите на кнопку **Настроить**. В случае успешного создания конфигурации отобразится соответствующее уведомление (рис. Успешное создание конфигурации 23).

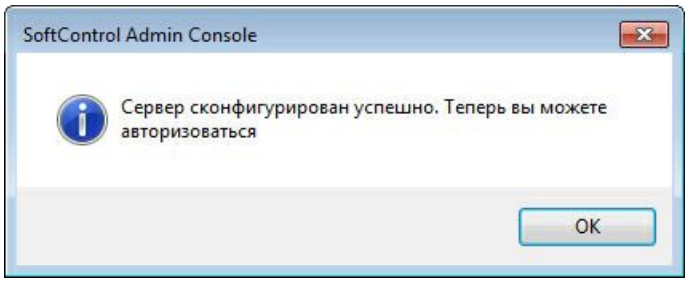


Рисунок 25. Успешное создание конфигурации

В окне авторизации[24] используйте данные созданной учётной записи для подключения к серверу SoftControl Server.

3.3 Регистрация клиентских приложений

После того как сервер прошел первичную настройку[19], на компьютере с установленным SoftControl Server формируется зашифрованный конфигурационный файл по следующему пути:

```
C:\ProgramData\SoftControl\ClientSettings.xmlc
```

Данный файл содержит параметры подключения клиентских приложений к серверу, а также общий клиентский сертификат[147], используемый по умолчанию для установления безопасного соединения. Для регистрации в SoftControl Service Center необходимо применить указанный файл на удалённых узлах ЛВС с предварительно установленными по документации клиентскими приложениями.

В режиме ожидания регистрации соединение с сервером осуществляется с использованием общего клиентского сертификата, при этом не происходит передача данных от клиента к серверу. Взаимодействие осуществляется в штатном режиме после перехода клиентского компонента в статус[39] **Активен**.

Подробные действия по применению файла описаны в документах «Руководство пользователя SoftControl ATM Client / Endpoint Client / SClient» и «Руководство по установке SoftControl DLP Client» для соответствующих компонентов.

3.4 Подключение к серверу из консоли управления

Для запуска консоли управления откройте ярлык SoftControl Admin Console на рабочем столе. В окне **Авторизация** введите **Адрес сервера**, **Имя пользователя** и **Пароль** (рис. Авторизация пользователя в SoftControl Admin Console[24]).

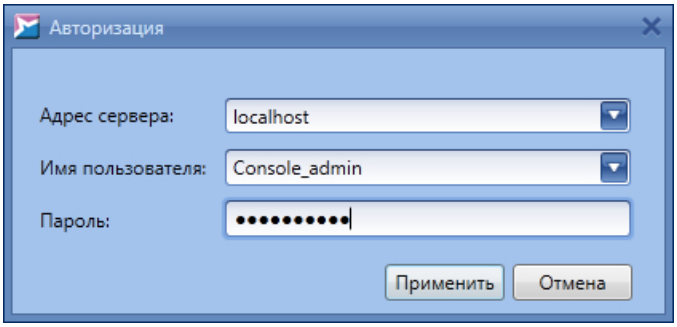


Рисунок 26. Авторизация пользователя в SoftControl Admin Console

Нажмите на кнопку **Применить**, чтобы подключиться к серверу SoftControl Server и приступить к централизованному управлению СИБ [26].

Для связи между SoftControl Admin Console и SoftControl Server по умолчанию используется порт *8080* протокола TCP. Если по какой-либо причине данный порт использовать не удаётся, измените его значение в файлах конфигурации серверного компонента и консоли управления.

Файл конфигурации сервера расположен по следующему пути:

`C:\ProgramData\SoftControl\Server.Config.xml`

Значение порта задаётся в атрибуте *Port* элемента *WebApiHost*.

Файл конфигурации консоли управления расположен по следующему пути:

`C:\ProgramData\SoftControl\SafenSoft.Enterprise.Console.exe.Config`

Значение порта задаётся в следующем участке файла:

```
<Databases>
  <Elements>
    <add name="<номер порта>" lastconnection="" />
  </Elements>
</Databases>
```

4. Централизованное управление СИБ

Удалённое централизованное управление клиентскими приложениями SoftControl SysWatch и SoftControl DLP Client осуществляется из консоли управления SoftControl Admin Console на базе сервисных функций, предоставляемых серверным компонентом SoftControl Server.

Данный раздел посвящен работе с SoftControl Admin Console и предназначен для администраторов системы информационной безопасности (далее по тексту – «СИБ») на основе SoftControl Service Center.

4.1 Интерфейс SoftControl Admin Console

Интерфейс консоли управления SoftControl Admin Console состоит из главного окна программы, в котором имеются следующие вкладки:

- Роли 30;
- Пользователи 33;
- События безопасности 35;
- Устройства и статусы 39;
- Подразделения 46;
- Настройки клиентов 52;
- Задачи 98;
- Лог 106;
- Сканнер 110;
- Измененные настройки 112;
- Контакты 125;
- Нотификации 126;
- Обновления 132.

В верхней части главного окна SoftControl Admin Console под основным меню программы расположен ряд графических кнопок, предназначенных для выполнения базовых операций при работе с SoftControl Admin Console. Кроме того, вкладки Устройства и статусы 39, Подразделения 46, Настройки клиентов 52, Задачи 98, Контакты 125 и Нотификации 126 имеют свои графические кнопки, область действия которых распространяется только на данные вкладки. Функции кнопок общего назначения описаны в табл. 5.

Таблица 5. Элементы управления SoftControl Admin Console общего назначения

Кнопка	Название	Описание	Горячие клавиши
	Сервер	Вызов настроек соединения с сервером.	
	Клиенты	Вызов вкладки **Устройства и статусы**.	F4
	Лог событий	Вызов вкладки **Лог** для всех клиентских компонентов.	
	Настройки клиентов	Вызов вкладки **Настройки клиентов**.	
	Подразделения	Вызов вкладки **Подразделения**.	
	Задачи	Вызов вкладки **Задачи**.	
	Нотификации	Вызов вкладки **Нотификации**.	
	Контакты	Вызов вкладки **Контакты**.	
	Роли	Вызов вкладки **Роли**.	
	Пользователи	Вызов вкладки **Пользователи**.	
	События безопасности	Вызов вкладки **События безопасности**.	
	Обновить	Обновление информации в текущей вкладке.	F5
	Выбрать колонки	Изменение состава полей таблицы текущей вкладки.	F6
	Сохранить настройки вида	Сохранение выбранного набора колонок в качестве пользовательского фильтра. Применима только к вкладке **Лог**.	F2
	Печать	Вывод текущего списка устройств или выборки событий на печать.	Ctrl + P
	Экспорт в Excel	Экспорт текущего списка устройств или выборки событий в файл формата *XLSX* (Microsoft® Excel®).	Ctrl + E
	Обновления	Вызов вкладки **Обновления**.	

Часть функций, вызываемых с помощью кнопок общего назначения, доступны также из главного меню программы.

В нижней части окна отображается строка с именем текущего пользователя и присущими ему ролями.

В главном окне SoftControl Admin Console дополнительно возможны следующие действия:

Настройка соединения с сервером

Если необходимо просмотреть или изменить параметры соединения консоли управления и сервера во время работы SoftControl Admin Console, нажмите на кнопку **Сервер**.

Окно настроек подключения аналогично окну авторизации[24], открываемому при запуске SoftControl Admin Console.

Настройка интерфейса

Для изменения настроек интерфейса SoftControl Admin Console в основном меню выберите пункт **Вид** → **Настройки**.

По умолчанию, язык интерфейса SoftControl Admin Console выбирается при первом запуске программы исходя из региональных настроек ОС. Для изменения языка в окне **Настройка интерфейса** выберите требуемый вариант из выпадающего списка (рис. Настройка интерфейса[28]):

- **ru-RU** – русский;
- **en-US** – английский (США).

Чтобы изменения вступили в силу, необходимо перезапустить программу.

Установите флажок **Запускать только один экземпляр консоли**, если необходимо запретить возможность одновременного запуска нескольких экземпляров SoftControl Admin Console.

В поле **Размер страницы событий** задаётся максимальное количество событий, которое должно отображаться на одной странице вкладки Лог[118].

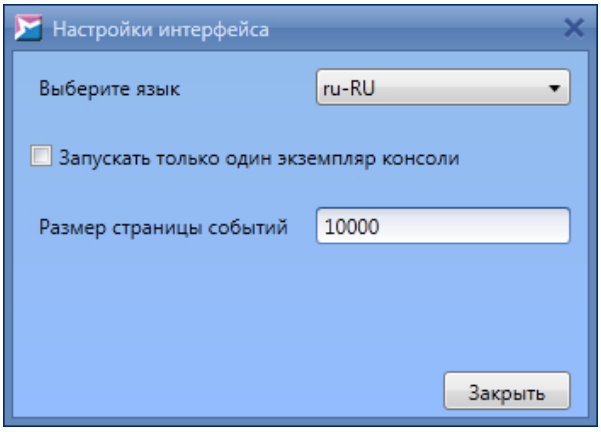


Рисунок 27. Настройка интерфейса

Просмотр информации о программе

В главном меню выберите пункт **О программе**.

4.2 Порядок работы

При администрировании СИБ на основе SoftControl Service Center из консоли управления SoftControl Admin Console рекомендуется придерживаться следующего порядка работы для снижения временных затрат и повышения продуктивности работы:

1) Откройте консоль управления SoftControl Admin Console, выполните подключение к серверу SoftControl Server [24].
2) На вкладке **Роли** при необходимости создайте дополнительные роли [30] и назначьте учётным записям [33] пользователей роли с выбранными разрешениями. С помощью вкладки **События безопасности** производите учёт действий пользователей [35] через консоль управления.
3) На вкладке **Устройства и статусы** подтвердите [43] или отклоните [43] запросы на регистрацию от клиентских приложений, установленных на конечных точках ЛВС.
4) После формирования рабочей области из необходимых устройств перейдите на вкладку **Настройки клиентов** и создайте необходимые конфигурации [53], которые будут применяться для клиентских приложений.
5) После создания клиентских настроек перейдите на вкладку **Подразделения** и создайте подразделения [48] (группы) по какому-либо принципу для распределения в них зарегистрированных компонентов на клиентских хостах. При создании подразделений выполните их привязку к определённым конфигурациям [49].
6) На вкладке **Устройства и статусы** переместите клиентские компоненты [45] в созданные подразделения.
7) На вкладке **Задачи** создайте необходимые задачи [98] для клиентских приложений.
8) Перейдите на вкладку **Лог** и приступите к просмотру отчётов клиентских компонентов [106].
9) Дополнительно можно настроить оповещения [126] об определённых событиях, которые будут отправляться на электронные почтовые ящики заданных адресатов [125], а также экспортировать и вывести на печать [123] необходимые данные.

4.3 Управление доступом на основе ролей

В SoftControl Service Center реализована подсистема управления доступом на основе ролей (*RBAC* – Role Based Access Control). Данная подсистема позволяет производить разграничение доступа пользователей [33] к различным функциям Сервисного Центра в зависимости от делегированной им роли [30].

При аутентификации пользователя на сервере создается сессия, имеющая уникальный идентификатор. Вся работа пользователя с консолью управления осуществляется в рамках данной сессии, при этом с постоянной периодичностью проверяется наличие соединения между сервером и консолью управления. Если консоль управления недоступна для сервера более чем 2 минуты, то текущая сессия прекращается.

Через SoftControl Admin Console осуществляется контроль действий пользователей с помощью регистрации событий безопасности сервера [35].

4.3.1 Роли

Вкладка **Роли** позволяет управлять ролями и настраивать разрешения для них (рис. Вкладка "Роли" [30]).

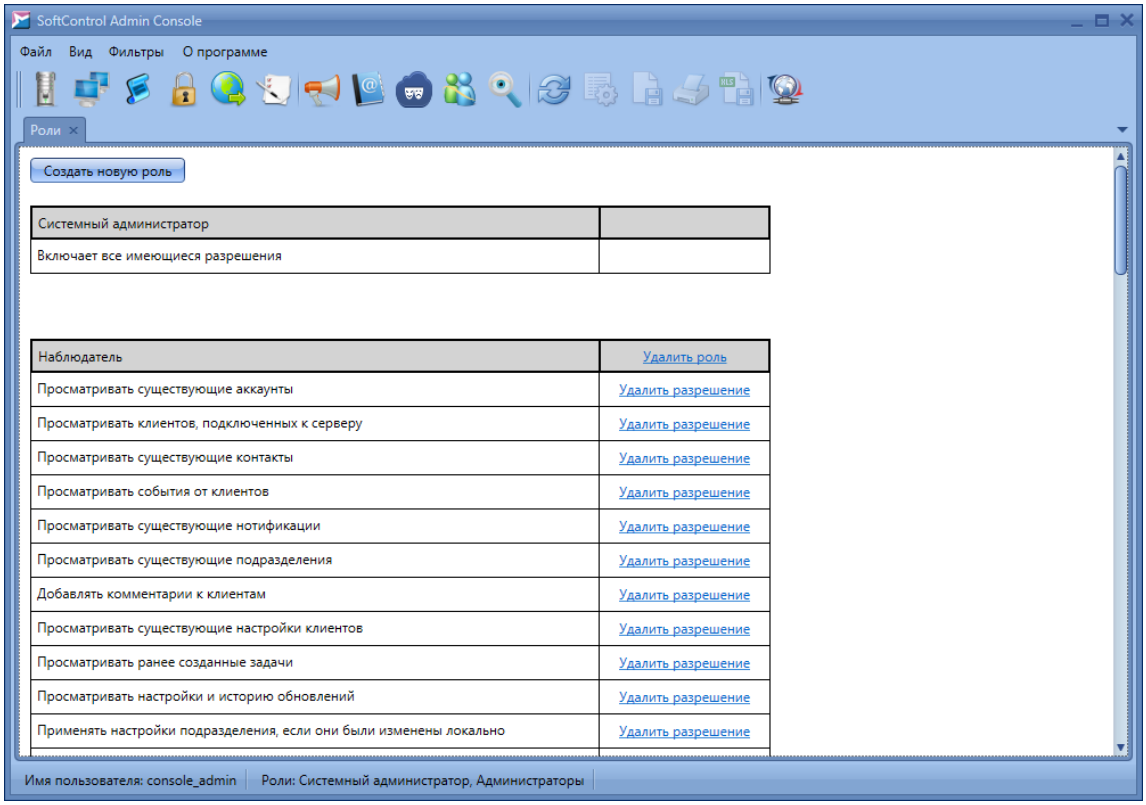


Рисунок 28. Вкладка "Роли"

Роли на вкладке представлены в виде таблиц, в первой строке которой указано имя роли, а в последующих – права на выполнение определённых операций в консоли управления (разрешения).

SoftControl Service Center включает в себя две предустановленные роли:

- **Системный администратор** – позволяет осуществлять доступ ко всей функциональности консоли управления. Рекомендуется для опытных пользователей/администраторов безопасности.
- **Наблюдатель** – дает права на просмотр основной части информации, включая все данные по работе с клиентскими приложениями. Рекомендуется для операторов, ведущих мониторинг инцидентов безопасности на клиентских хостах.

Помимо этого, можно создать новые роли с собственным набором разрешений. Ниже описаны действия с ролями, выполняемые на данной вкладке:

Создание роли

Чтобы добавить роль, нажмите на кнопку **Создать новую роль** (рис. Вкладка "Роли" 30). В появившемся окне укажите **Имя роли** и нажмите на кнопку **OK** (рис. Создание новой роли 31).

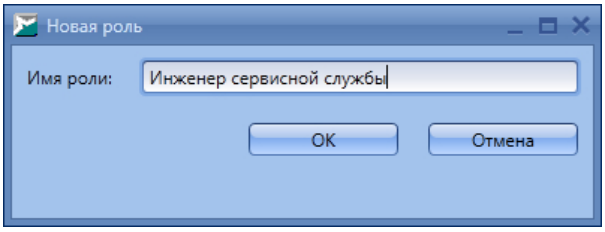


Рисунок 29. Создание новой роли

Новая роль будет добавлена в конец списка ролей. Далее задайте разрешения 31 для неё.

Редактирование разрешений

Чтобы добавить разрешения к роли, нажмите на кнопку **Добавить разрешение** после таблицы с данной ролью. В появившемся окне отметьте необходимые разрешения и нажмите на кнопку **OK** (рис. Добавление разрешений 31).

Чтобы удалить разрешение, нажмите на ссылку **Удалить разрешение** в соответствующей строке таблицы с ролью (рис. Вкладка "Роли" 30).

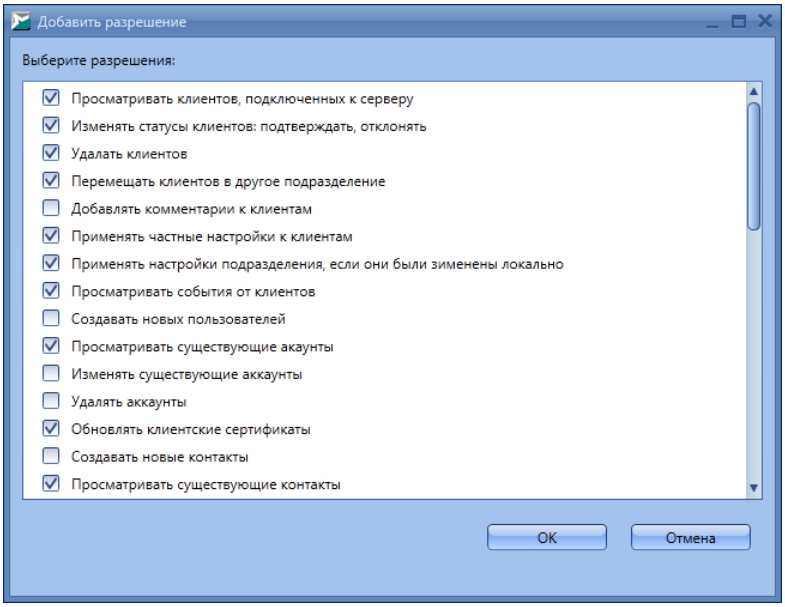


Рисунок 30. Добавление разрешений

Удаление роли

Для удаления роли нажмите на ссылку **Удалить роль** в строке таблицы с именем роли (рис. Вкладка "Роли" 30) и подтвердите удаление в диалоговом окне.

4.3.2 Пользователи

На вкладке **Пользователи** производится управление учётными записями пользователей и назначение ролей для них (рис. Вкладка "Пользователи" 33).

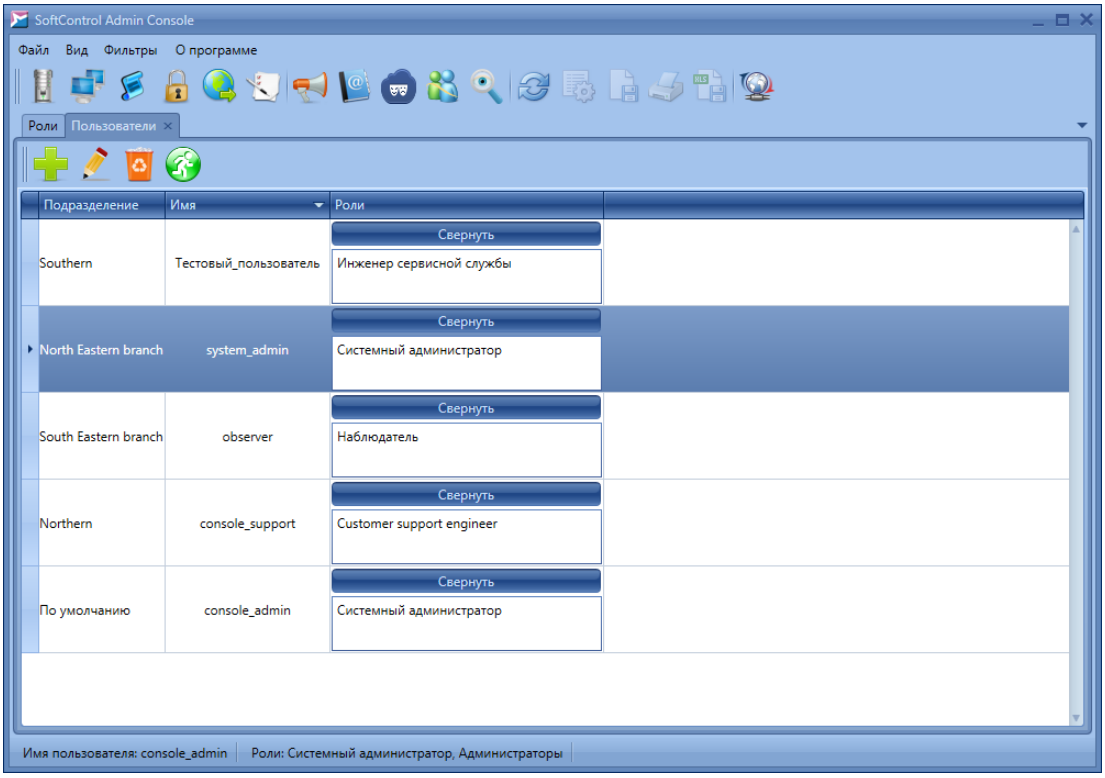


Рисунок 31. Вкладка "Пользователи"

Основные операции с учётными записями пользователей осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 6.

Таблица 6. Элементы управления вкладки "Пользователи"

Кнопка	Название	Описание
	Создать	Создание новой учётной записи.
	Правка	Редактирование свойств выбранной учётной записи.
	Удалить	Удаление выбранных учётных записей.
	Переместить	Переместить выбранного пользователя в другое подразделение.

Перечень полей вкладки приведён в табл. 7.

Таблица 7. Поля вкладки "Пользователи"

Поле	Описание
Подразделение	Подразделение, к которому приписан данный пользователь.

Поле	Описание
Имя	Имя пользователя.
Роли	Роли, присущие пользователю.

Основные действия, выполняемые на данной вкладке:

Создание учётной записи

Чтобы добавить новую учётную запись, нажмите на кнопку **Создать** (рис. Вкладка "Пользователи" 33). В появившемся окне укажите **Имя** пользователя, введите **Пароль** учётной записи и его **Подтверждение** (не менее 7 символов). Укажите необходимые **Роли** для создаваемого пользователя и нажмите на кнопку **Применить** (рис. Создание учётной записи 34).

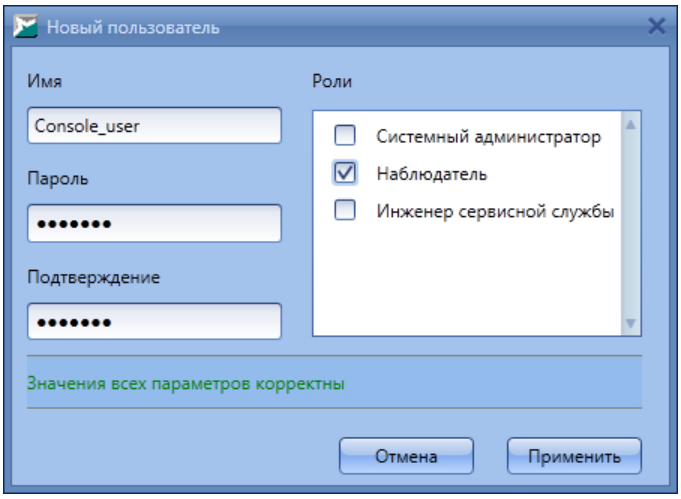


Рисунок 32. Создание учётной записи

Все новые учётные записи автоматически помещаются в отделение **По умолчанию**. Вы можете переместить 35 выбранную учётную запись в другое подразделение.
В зависимости от роли 30, пользователь имеет доступ к информации в текущем подразделении и во всех дочерних подразделениях и не имеет доступа к информации в родительских подразделениях.

Редактирование учётной записи

Чтобы изменить свойства учётной записи, нажмите на кнопку **Правка** (рис. Вкладка "Пользователи" 33).
В появившемся окне измените **Имя** пользователя и/или измените **Роли** в соответствующей области, после чего нажмите на кнопку **Применить**

(рис. Редактирование учётной записи[35]). Пароль при этом останется без изменений. Если требуется сменить пароль, то введите новый **Пароль** в одноименном поле и его **Подтверждение** (не менее 7 символов).

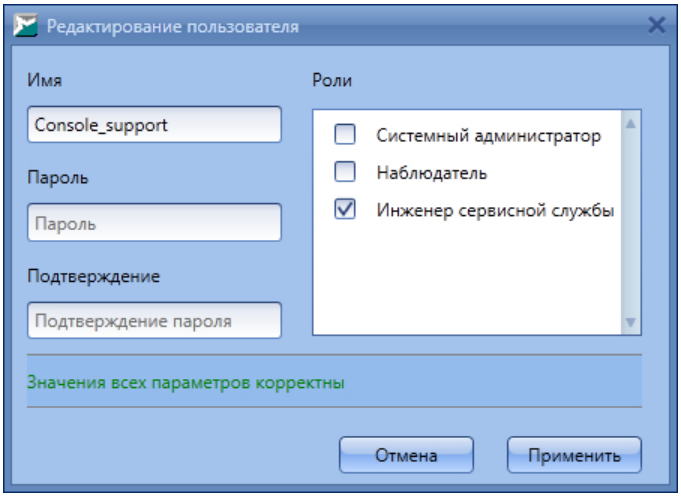


Рисунок 33. Редактирование учётной записи

Удаление учётной записи

Для удаления учётной записи выберите её, нажмите на кнопку **Удалить** (рис. Вкладка "Пользователи"[33]) и подтвердите удаление в диалоговом окне.

Перемещение учётной записи

Для перемещения учётной записи выберите её, нажмите на кнопку **Переместить** и в появившемся окне укажите подразделение, в которое надо переместить данного пользователя (рис. Перемещение учётной записи[35]).

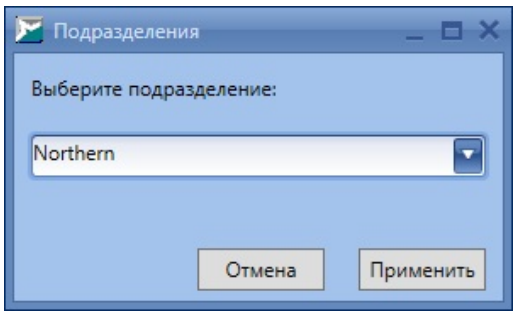


Рисунок 34. Перемещение учётной записи

4.3.3 События безопасности сервера

Консоль управления позволяет фиксировать операции, производимые пользователями, для дальнейшего анализа на вкладке **События безопасности** (рис. Вкладка "События

безопасности" [37]).

Полный перечень полей вкладки приведён в табл. 8.

Таблица 8. Поля вкладки "События безопасности"

Поле	Описание
Guid клиента	Уникальный идентификатор клиентского приложения (только для типов событий **Подтверждение клиента**, **Отклонение клиента**, **Удаление клиента**, **Перемещение клиента в другое подразделение**).
Тип события	Тип зарегистрированного события: • **Начало сессии**; • **Конец сессии**; • **Роль создана**; • **Роль удалена**; • **К роли добавлены разрешения**; • **Удалено разрешение у роли**; • **Была создана учетная запись**; • **Учетная запись была изменена**; • **Учетная запись была удалена**; • **Подтверждение клиента**; • **Отклонение клиента**; • **Удаление клиента**; • **Запрос на изменение сертификата клиента**; • **Новый сертификат назначен клиенту**; • **Перемещение объекта в другое подразделение**; • **Создано новое подразделение**; • **Подразделение было удалено**; • **Создание новых настроек**; • **Изменение настроек для подразделения**; • **Применение частных настроек**; • **Удалено хранилище настроек**; • **Назначено частное хранилище настроек**; • **Создание задачи**; • **Отмена задачи**; • **Создан контакт**; • **Контакт изменен**; • **Контакт был удален**; • **Была создана нотификация**; • **Нотификация была изменена**; • **Нотификация была удалена**; • **Неавторизованный запрос**; • **Недостаточно прав на выполнение запроса**; • **Ошибка обработки запроса**.
Тип задачи	Тип задачи (только для типов событий **Создание задачи**, **Отмена задачи**).
Сообщение об ошибке	Сообщение об ошибке во время обработки запроса.
Причина ошибки авторизации	Причина невозможности авторизации на сервере (только для типа события **Неавторизованный запрос**).
ID задачи	Порядковый номер задачи (только для типов событий **Создание задачи**, **Отмена задачи**).

Поле	Описание
Номер порта запроса	Порт компьютера с установленной консолью управления SoftControl Admin Console, от которой пришел запрос на сервер.
URI запроса	Полный URI запроса консоли управления SoftControl Admin Console, который был отправлен на сервер.
Имя подразделения	Подразделение, в которое перемещён установленный клиентский компонент (только для типов событий **Перемещение клиента в другое подразделение**, **Создано новое подразделение**, **Подразделение было удалено**).
Разрешения роли	Перечисление добавленных (для типа события **К роли добавлены разрешения**) или удаленных (для типа события **Удалено разрешение у роли**) разрешений роли.
ID сессии	Контрольная сумма идентификатора сессии, с которой ассоциировано событие.
Имя аккаунта	Имя учётной записи пользователя (только для типов событий **Была создана учетная запись**, **Учетная запись была изменена**, **Учетная запись была удалена**).
Имя роли	Имя роли (только для типов событий **Роль создана**, **Роль удалена**, **К роли добавлены разрешения**, **Удалено разрешение у роли**).
Имя пользователя	Имя пользователя, с которым ассоциировано данное событие.
Имя нотификации	Имя оповещения (только для типов событий **Была создана нотификация**, **Нотификация была изменена**, **Нотификация была удалена**).
Имя настроек	Имя конфигурации клиентских приложений (только для типов событий **Создание новых настроек**, **Изменение настроек для подразделения**, **Удалено хранилище настроек**).
Имя контакта	Имя адресата получателя оповещений (только для типов событий **Создан контакт**, **Контакт был изменен**, **Контакт был удален**).
Время возникновения	Дата и время возникновения события.
Время создания настроек	Время создания настроек клиентских приложений на сервере (только для типа события **Создание новых настроек**).
Имя клиента	NetBIOS-имя клиентского хоста (только для типов событий **Подтверждение клиента**, **Отклонение клиента**, **Удаление клиента**, **Запрос на изменение сертификата клиента**, **Новый сертификат назначен клиенту**, **Перемещение клиента в другое подразделение**).
IP адрес запроса	IP-адрес компьютера с установленной консолью управления SoftControl Admin Console, от которой пришел запрос на сервер.

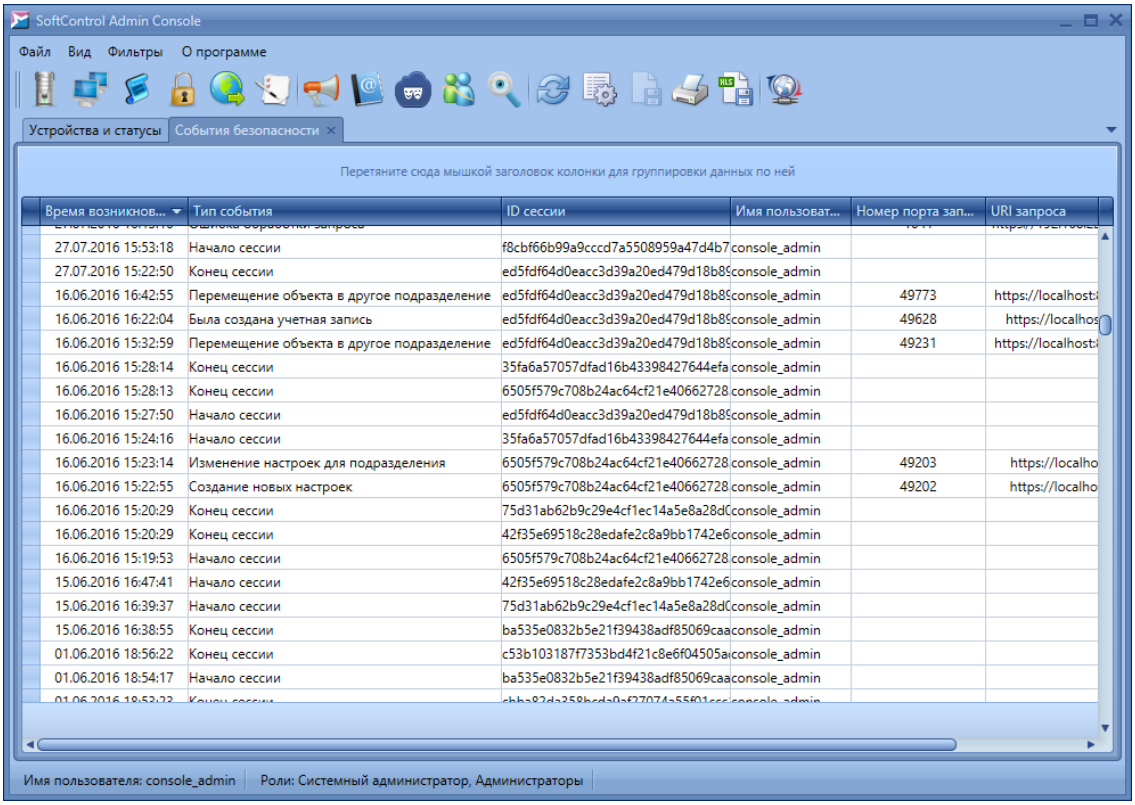


Рисунок 35. Вкладка "События безопасности"

Дополнительные действия, возможные на данной вкладке:

Изменение состава колонок

Если необходимая колонка отсутствует в заголовке таблицы, то для добавления нового поля нажмите кнопку **Выбрать колонки** и перетащите требуемое поле из окна **Выбор колонок** (рис. Выбор колонок 38) в необходимое место заголовка таблицы. Для удаления существующего поля перетащите его в окно **Выбор колонок**, либо за пределы заголовка таблицы.

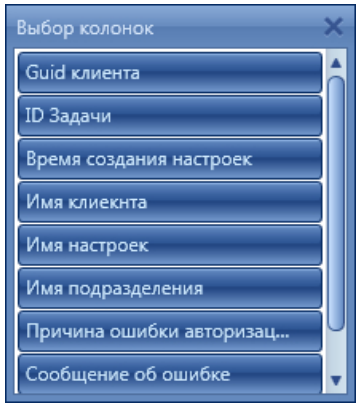


Рисунок 36. Выбор колонок

Группировка данных

Информация на вкладке может группироваться по всем полям (категориям), кроме поля **Время возникновения**, для удобства просмотра. Для группировки по категориям перетащите заголовок колонки на панель, расположенную между заголовком таблицы и группой кнопок вкладки (рис. Вкладка "События безопасности" 37). Если группировка производится по нескольким категориям, то приоритет (вложенность категорий) уменьшается слева направо в зависимости от расположения на панели.

4.4 Устройства и статусы

Вкладка **Устройства и статусы** служит для управления регистрацией клиентских приложений, перемещением их в подразделения, отслеживания статуса и получения информации о хостах, на которых они установлены (рис. Вкладка "Устройства и статусы" 39).

Основные операции с клиентскими компонентами осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 9.

Таблица 9. Элементы управления вкладки "Устройства и статусы"

Кнопка	Название	Описание	Горячие клавиши
	Одобрить	Одобрение регистрации клиентского компонента на сервере.	
	Отклонить	Отклонение регистрации клиентского компонента на сервере.	
	Сертификат	Обновление индивидуального сертификата клиентского компонента.	
	Удалить клиентов	Удаление выбранных клиентских компонентов из БД.	Delete
	Переместить	Перемещение выбранных клиентских компонентов в другое подразделение.	
	Лог событий	Вызов вкладки **Лог** для выбранных компонентов.	

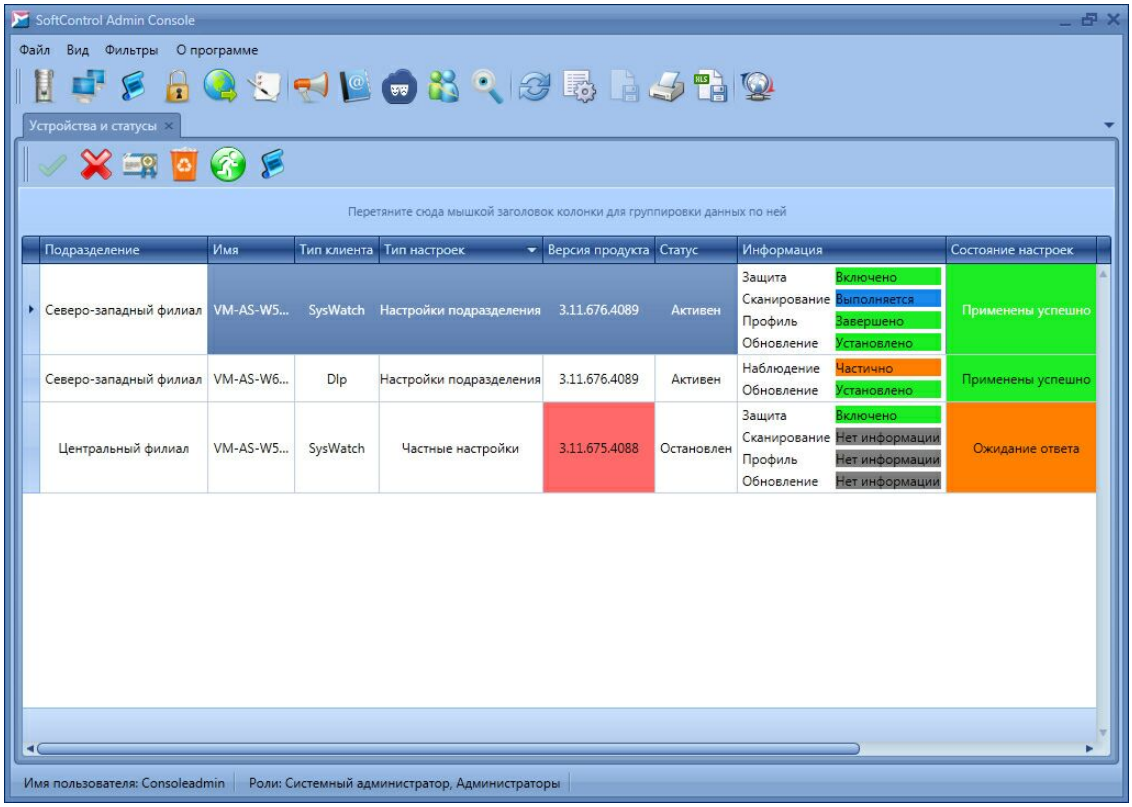


Рисунок 37. Вкладка "Устройства и статусы"

Полный перечень полей вкладки приведён в табл. 10.

Таблица 10. Поля вкладки "Устройства и статусы"

Поле	Описание
Подразделение	Подразделение, к которому принадлежит клиентский компонент.
Имя	NetBIOS-имя клиентского хоста.
Тип клиента	Тип установленного клиентского компонента на данном клиентском хосте: • **SysWatch** – компонент проактивной защиты (SoftControl ATM Client / Endpoint Client / SClient); • **DLP** – компонент сбора данных (SoftControl DLP Client).
Тип настроек	Тип конфигурации клиентского компонента: • **Настройки подразделения** – настройки, общие для подразделения, которому принадлежит клиентский компонент; • **Частные настройки** – настройки, индивидуальные для клиентского компонента, независимо от подразделения; • **Локальные настройки** – настройки, изменённые локально для клиентского компонента типа SysWatch.
Версия продукта	Версия установленного клиентского компонента. Если версия компонента ниже версии SoftControl Admin Console, данная ячейка подсвечивается красным цветом, если выше – оранжевым.
Статус	Возможные статусы, отражающие текущее состояние клиентского компонента: • **Ожидает решения**: от клиентского приложения получен запрос на регистрацию, ожидается решение администратора. • **Одобрен**: запрос на регистрацию от клиентского приложения одобрен администратором.

Поле	Описание
	• **Отклонен**: запрос на регистрацию от клиентского приложения отклонен администратором. • **Активен**: за последний отрезок времени, равный удвоенному значению интервала обращения клиента к серверу [56], зафиксирован факт установки связи зарегистрированного клиентского приложения с сервером. • **Остановлен**: за последний отрезок времени, равный удвоенному значению интервала обращения клиента к серверу [56], не зафиксирован факт установки связи зарегистрированного клиентского приложения с сервером.
Информация	Дополнительная информация по состоянию клиентского компонента. Для компонента типа **SysWatch** имеет следующие показатели: • **Защита** – статус проактивной защиты. – **Включено**: защита включена по всем областям контроля; – **Отключено**: защита отключена по всем областям контроля; – **Частично**: защита включена по части областей контроля. • **Сканирование** – статус последней по времени задачи антивирусного сканирования. • **Профиль** – статус последней по времени задачи сбора профиля (автоматической настройки). – **Выполняется**: задача находится в процессе выполнения; – **Остановлено**: задача остановлена пользователем; – **Завершено**: задача успешно завершена; – **Ошибка**: возникла ошибка в процессе запуска или завершения задачи. • **Обновление** – статус последнего по времени обновления компонента. – **Установлено**: обновление было успешно установлено; – **Не найдено**: обновления для компонента не найдены; – **Перезагрузить**: необходима перезагрузка клиентского хоста для завершения обновления. Статус **Нет информации** для операций **Сканирование**, **Профиль** и **Обновление** означает, что указанные действия не производились с момента регистрации клиентского приложения на сервере. Для компонента типа **DLP** имеет следующие показатели: • **Наблюдение** – статус активности наблюдения. – **Включено**: наблюдение включено по всем областям сбора данных (не включает в себя подкатегорию съёмных носителей); – **Отключено**: наблюдение отключено по всем областям сбора данных; – **Частично**: наблюдение включено по части областей сбора данных.
Изменён	Время регистрации последнего события выбранным клиентским компонентом.
IP адрес	IP-адрес клиентского хоста.
DNS	Сетевое имя клиентского хоста в рабочей группе либо доменной сети.
Количество дней до окончания лицензии	Количество дней, оставшихся до истечения срока действия текущего лицензионного ключа клиентского приложения.
Состояние настроек	Статус применения настроек клиентского приложения, полученных им со стороны сервера SoftControl Server. Обновляется динамически при каждом изменении настроек через консоль управления SoftControl Admin Console. Возможные состояния: • **применены успешно**; • **ожидание ответа**; • **ошибка применения**;

Поле	Описание
	• **локальные настройки**; • **нет информации**.
Срок действия сертификата	Дата, до которой действителен индивидуальный сертификат клиентского приложения.
Комментарий	Поле для ввода комментария к выбранному клиентскому компоненту.
Уникальный ID устройства	Уникальный идентификатор клиентского компонента, который автоматически присваивается ему при первом обращении к серверу SoftControl Server.

Основные действия, выполняемые на данной вкладке:

- управление процессом регистрации [43];
- перемещение в подразделения [45];
- управление списком файлов, разрешённых к запуску [45].

Дополнительные действия, возможные на данной вкладке:

Работа с несколькими компонентами

Вкладка позволяет работать как с одним, так и с несколькими клиентскими компонентами. Для выполнения действий над несколькими компонентами выберите их с помощью одного из способов выделения и произведите требуемые действия:

- выделение нескольких произвольных компонентов: зажмите клавишу **Ctrl** на клавиатуре и выделите требуемые компоненты;
- выделение диапазона компонентов: выберите первый компонент диапазона, зажмите клавишу **Shift** на клавиатуре и выберите последний компонент диапазона.

Группировка данных

Информация на вкладке может группироваться по определённым полям для удобства отображения. Полями, по которым возможно произвести группировку (категориями), являются **Подразделение**, **Тип клиента**, **Тип настроек**, **Версия продукта**, **Статус**, **IP адрес**, **DNS**, **Количество дней до окончания лицензии**, **Состояние настроек** и **Комментарий**. Для группировки по указанным категориям перетащите заголовок колонки на панель, расположенную между заголовком таблицы и группой кнопок вкладки (рис. Вкладка "Устройства и статусы" [39]). Если группировка производится по нескольким категориям, то приоритет (вложенность категорий) уменьшается слева направо в зависимости от расположения на панели.

Просмотр отчётов

Для открытия вкладки Лог[106] со списком событий выделите требуемые компоненты и выполните одно из следующих действий:

- нажмите на кнопку **Лог событий** в группе кнопок вкладки (рис. Вкладка "Устройства и статусы"[39]);
- вызовите контекстное меню нажатием правой кнопки мыши на списке компонентов и выберите команду **Показать события**.

При открытии списка событий в заголовке вкладки Лог[106] отображается количество выбранных компонентов (рис. Вкладка "Устройства и статусы"[39]).

4.4.1 Управление процессом регистрации

Управление процессом регистрации включает в себя следующие действия:

Подтверждение регистрации

Выберите в списке требуемые клиентские компоненты, находящиеся в состоянии **Ожидает решения**, и нажмите на кнопку **Одобрить** (рис. Вкладка "Устройства и статусы"[39]).

Поле **Статус** после подтверждения регистрации выбранных клиентов изменяет свое состояние на **Одобрен**.

При следующем получении запроса от клиентского компонента происходит проверка его сертификата[147]: если он общий, то серверный компонент SoftControl Server выдает индивидуальный сертификат для авторизации на сервере. При следующем обращении клиентского компонента (с индивидуальным сертификатом) его статус изменяется на **Активен**. С этого момента клиентский компонент считается введённым в эксплуатацию: между сервером и клиентом установлен безопасный зашифрованный канал связи.

Отклонение регистрации

Выберите в списке требуемые клиентские компоненты, находящиеся в состоянии **Ожидает решения**, и нажмите на кнопку **Отклонить** (рис. Вкладка "Устройства и статусы"[39]).

Поле **Статус** после отклонения регистрации выбранных клиентов изменяет свое состояние на **Отклонен**.

При переходе в это состояние клиентский сертификат помещается в черный список и дальнейшее взаимодействие с сервером прекращается.

После отклонения регистрации повторную попытку можно совершить только следующим образом:

1) Удалите клиентские компоненты из БД с помощью кнопки **Удалить клиентов**.
2) Повторите процедуру регистрации на сервере с общим сертификатом[147].

Обновление клиентского сертификата

Выберите в списке требуемые клиентские компоненты, находящиеся в состоянии **Активен** или **Остановлен**, и нажмите на кнопку **Сертификат** (рис. Вкладка "Устройства и статусы"[39]).

Поле **Срок действия сертификата** обновляется после следующего обращения клиентского компонента с новым индивидуальным сертификатом[147]. При этом использование предыдущего сертификата становится невозможным в связи с его помещением в чёрный список.

Удаление клиентского компонента из БД

Выберите в списке требуемые клиентские компоненты и нажмите на кнопку **Удалить клиентов** (рис. Вкладка "Устройства и статусы"[39]). При этом не происходит отзыва клиентского сертификата[147] и через интервал обращения клиента к серверу в консоли управления SoftControl Admin Console вновь отобразятся удалённые компоненты в статусе **Ожидает решения**. Для полного вывода клиентских компонентов из эксплуатации необходима следующая последовательность действий:

1) Поместите индивидуальный сертификат[147] клиентского компонента в чёрный список с помощью кнопки **Отклонить**.
2) Удалите клиентские компоненты из БД с помощью кнопки **Удалить клиентов**.

4.4.2 Перемещение в подразделения

Для перемещения выбранных клиентских компонентов в другое подразделение, нажмите на кнопку **Переместить** и в появившемся окне выберите из выпадающего списка необходимое подразделение (рис. Выбор подразделения для перемещения компонента 45).

При перемещении клиентских компонентов в другое подразделение их настройки автоматически изменяются на конфигурацию данного подразделения.

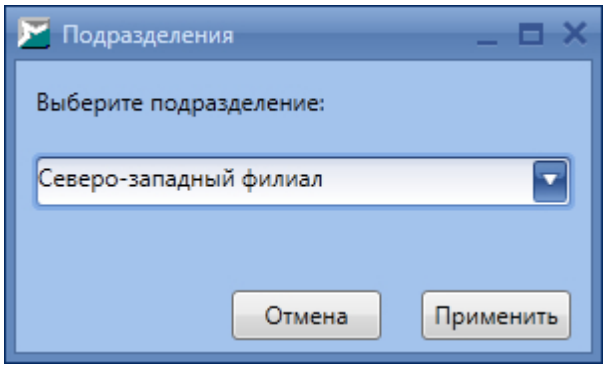


Рисунок 38. Выбор подразделения для перемещения компонента

4.4.3 Управление списком разрешённых файлов

SoftControl Admin Console позволяет получить список файлов, разрешённых к запуску на компьютере с установленным клиентским приложением SoftControl SysWatch, и при необходимости отозвать разрешения для выбранных файлов.

Для получения списка файлов щёлкните правой кнопкой мыши по требуемому клиентскому приложению SoftControl SysWatch и в контекстном меню выберите команду **Просмотр данных профиля**. Данное действие открывает вкладку **Данные профиля для <имя_клиентского_приложения>** (рис. Вкладка "Данные профиля для..." 45). Для начала сбора профиля нажмите на кнопку **Запросить обновление**. В процессе сбора данных SoftControl Admin Console показывает примерное время до окончания сбора. Список файлов содержит следующую дополнительную информацию: имя файла в момент добавления в список, его контрольная сумма, полный путь, дата добавления и размер.

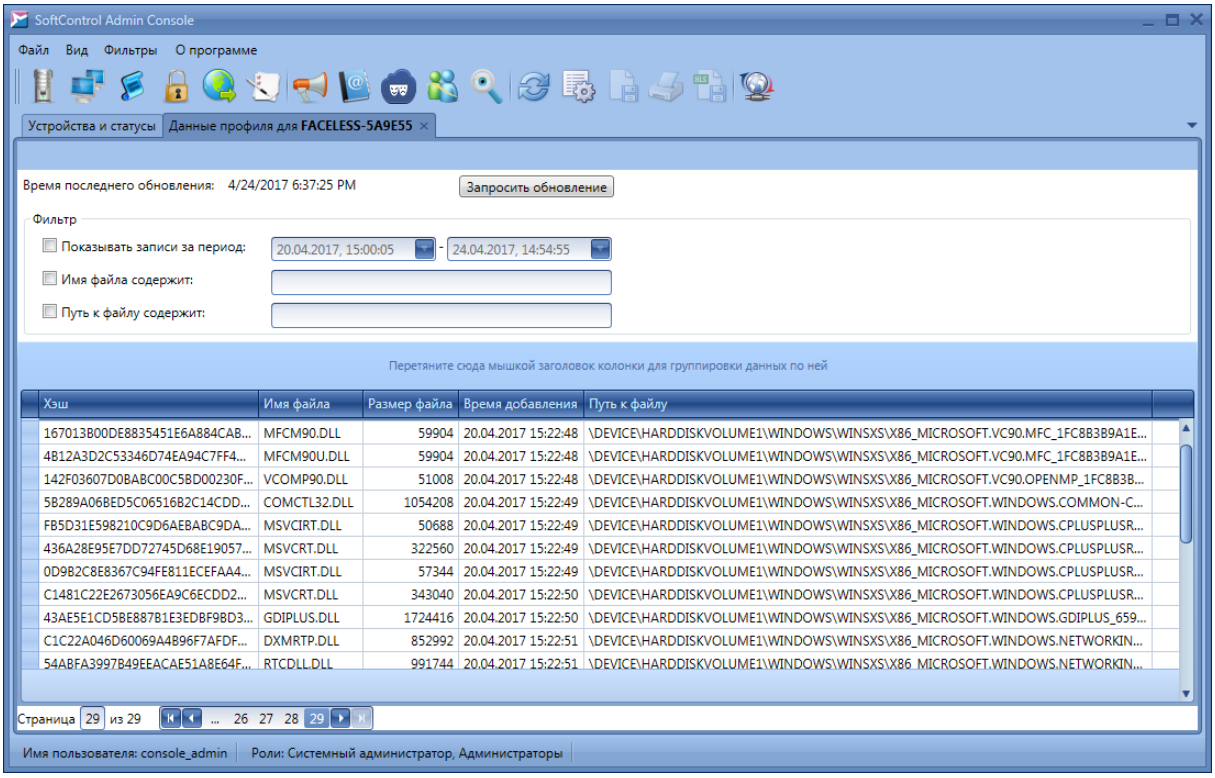


Рисунок 39. Вкладка "Данные профиля для..."

Для просмотра списка файлов за определённый период времени выберите требуемые даты в поле **Фильтр**. Вы также можете указать в фильтре часть имени файла и пути к нему. Для того чтобы отозвать разрешения на запуск для каких-либо файлов, выделите их, используя клавиши **Shift** и **Ctrl**, и в контекстном меню выберите команду **Удалить выбранные**.

4.5 Подразделения

Вкладка **Подразделения** предназначена для группирования клиентских компонентов по территориальному, административному или иному признаку (рис. Вкладка "Подразделения" 46). Кроме того, на вкладке производится привязка подразделений к определённым наборам настроек и генерация одноразовых паролей.

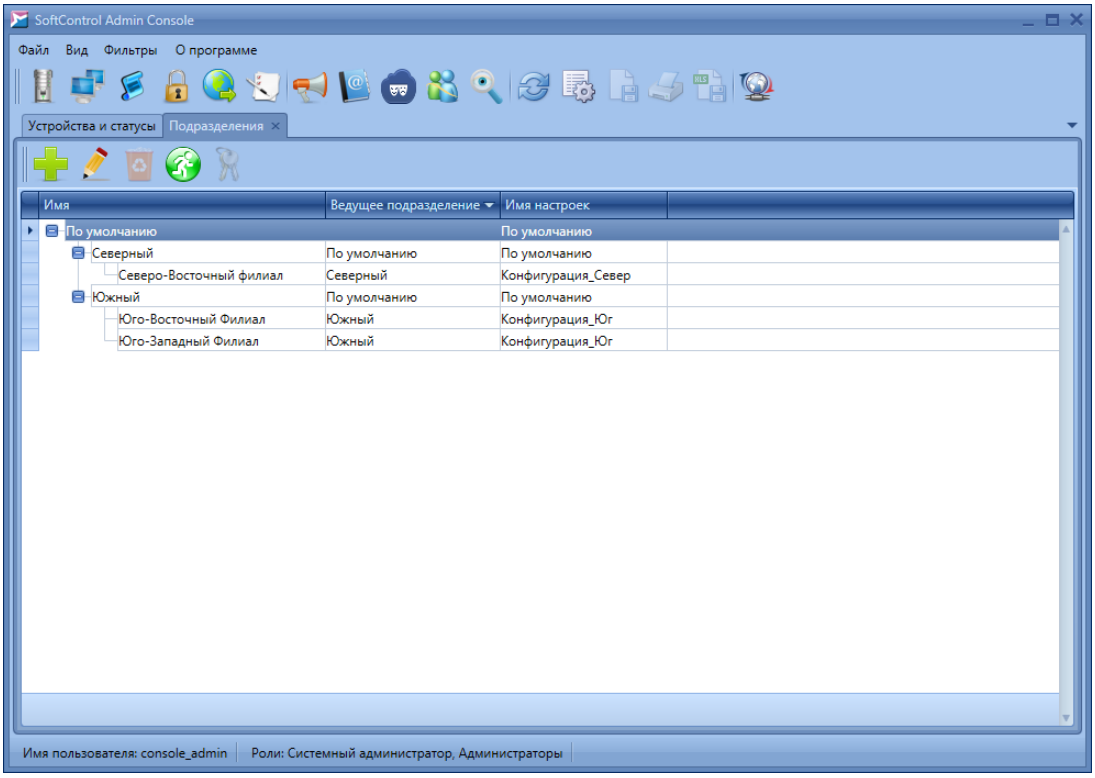


Рисунок 40. Вкладка "Подразделения"

В программе всегда существует как минимум одно подразделение – **По умолчанию**; его удаление невозможно. Все новые клиентские компоненты автоматически помещаются в данное подразделение. В дальнейшем администратор может создать требуемую иерархическую структуру подразделений (с любым уровнем вложенности), используя кнопку **Переместить**. Каждому подразделению при создании назначается конфигурация (настройки) клиентских приложений.

Основные операции с подразделениями осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 11.

Таблица 11. Элементы управления вкладки "Подразделения"

Кнопка	Название	Описание
	Создать	Создание нового подразделения.
	Правка	Редактирование свойств выбранного подразделения.
	Удалить	Удаление выбранных подразделений.
	Переместить	Переместить выбранное подразделение в другое. Нельзя перемещать подразделение **По умолчанию**, а также родительское подразделение в дочернее.
	Одноразовый пароль	Открытие окна генератора одноразовых паролей.

Перечень полей вкладки приведён в табл. 12.

Таблица 12. Поля вкладки "Подразделения"

Поле	Описание
Имя	Наименование подразделения.
Ведущее подразделение	Наименование родительского подразделения.
Имя настроек	Наименование конфигурации клиентских компонентов, действующее в выбранном подразделении.

Основные действия, выполняемые на данной вкладке:

- управление подразделениями [48];
- генерация одноразовых паролей [50].

4.5.1 Управление подразделениями

Управление подразделениями включает в себя следующие действия:

Создание подразделения

Чтобы добавить новое подразделение, нажмите на кнопку **Создать** (рис. Вкладка "Подразделения" [46]). В появившемся окне укажите **Имя** подразделения и выберите **Имя настроек** в выпадающем списке, после чего нажмите на кнопку **Применить** (рис. Создание подразделения [48]).

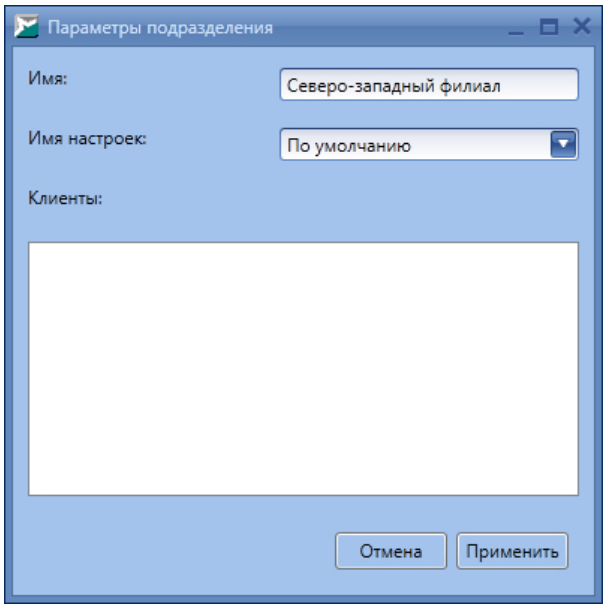


Рисунок 41. Создание подразделения

Изменение свойств подразделения

Чтобы изменить свойства подразделения, нажмите на кнопку **Правка** (рис. Вкладка "Подразделения" 46).

В появившемся окне измените **Имя** подразделения и/или выберите другое **Имя настроек** в выпадающем списке, после чего нажмите на кнопку **Применить** (рис. Параметры подразделения 49). Если данное подразделение содержит компоненты, их перечень отображается в списке **Клиенты**.

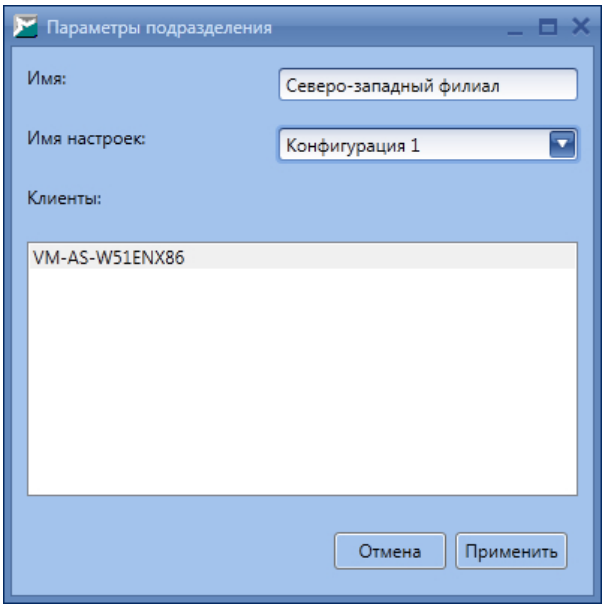


Рисунок 42. Параметры подразделения

Удаление подразделения

Для удаления подразделения выберите его, нажмите на кнопку **Удалить** (рис. Вкладка "Подразделения" 46) и подтвердите удаление в диалоговом окне.

Удаление подразделения **По умолчанию** невозможно.

Перемещение подразделения

Для перемещения подразделения выберите его, нажмите на кнопку **Переместить** и в появившемся окне укажите подразделение, в которое происходит перемещение (рис. Перемещение подразделения 49).

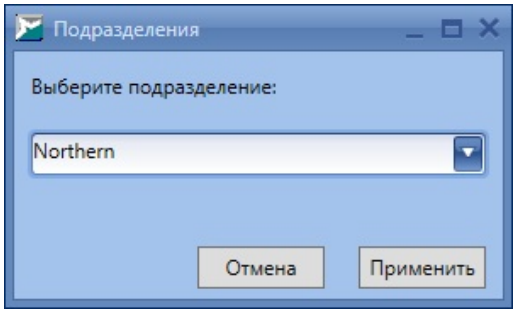


Рисунок 43. Перемещение подразделения

Невозможно переместить подразделение **По умолчанию**, а также родительское подразделение в дочернее.

4.5.2 Генерация одноразовых паролей

В SoftControl Service Center реализована подсистема защищенной аутентификации на основе алгоритма создания одноразовых паролей. Данный алгоритм обладает высокой криптографической стойкостью и позволяет генерировать пароли, действительные только в течение определённого промежутка времени. Одноразовые пароли могут быть использованы для доступа к ГИП/деинсталлятору клиентского компонента SoftControl SysWatch в случае необходимости (например, если требуется обеспечить однократный доступ к SoftControl SysWatch без раскрытия основного пароля).

Для начала работы с генератором одноразовых паролей необходимо, чтобы в текущей конфигурации подразделения была включена и настроена соответствующая опция (68).

Генерация одноразовых паролей осуществляется в рамках подразделения: создаваемый пароль применим для всех клиентских приложений SoftControl SysWatch, входящих в подразделение. Выберите подразделение и нажмите на кнопку **Одноразовый пароль**, чтобы открыть окно генератора (рис. Вкладка "Подразделения" (46)). В появившемся окне отображается **Текущий пароль** и его время жизни в счётчике **Осталось времени** в формате *дд:чч:мм:сс* (рис. Окно генерации (51)). По истечении интервала времени жизни **Текущий пароль** обновляется.

l) Использование одноразовых паролей рассчитано на применение совместно с основным паролем. Для возможности получения доступа к SoftControl SysWatch на клиентском хосте по одноразовым паролям должна быть включена общая

парольная защита[63]. При запросе пароля в ГИП SoftControl SysWatch необходимо установить флажок **Использовать одноразовый пароль**.

II) В связи с тем, что алгоритм создания одноразовых паролей в качестве параметра принимает время, для его корректной работы необходимо, чтобы время по UTC (т.е. независимо от часового пояса) на компьютере с SoftControl Admin Console и хосте с установленным SoftControl SysWatch было синхронизировано с погрешностью, значительно меньшей времени жизни пароля.

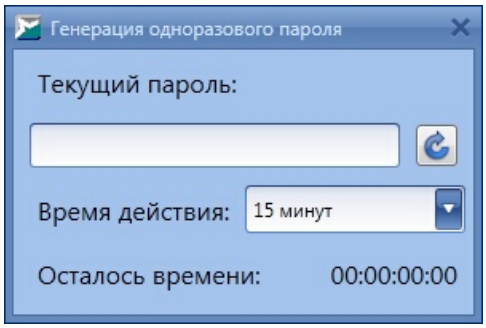


Рисунок 44. Окно генерации

4.6 Настройка клиентских приложений

Вкладка **Настройки клиентов** содержит список конфигураций (наборов настроек) клиентских приложений (рис. Вкладка "Настройки клиентов" 52).

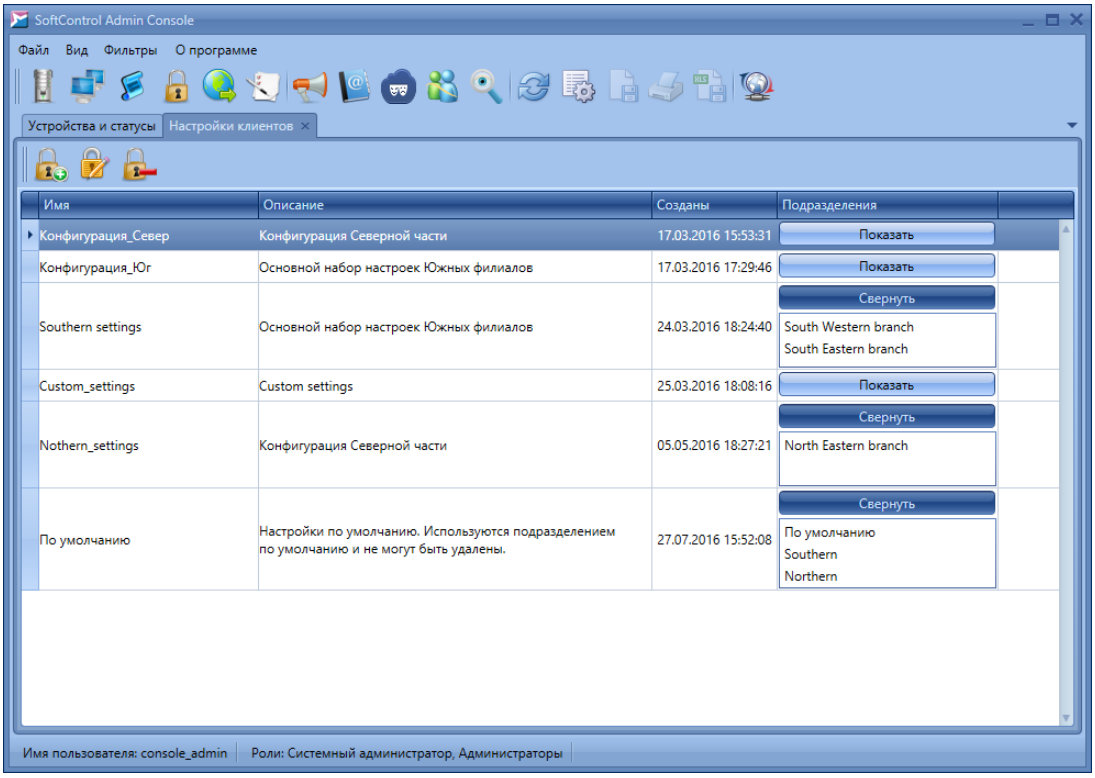


Рисунок 45. Вкладка "Настройки клиентов"

В SoftControl Admin Console различаются следующие типы конфигураций:

- настройки подразделения;
- частные настройки;
- локальные настройки (только для SoftControl SysWatch).

По умолчанию, все клиентские компоненты после регистрации на сервере получают настройки подразделения. Частные настройки созданы для тех случаев, когда требуется задать для определенного клиентского компонента конфигурацию, отличную от конфигурации подразделения. На вкладке отображается список всех конфигураций, включая частные. Информация по работе с частными настройками приведена ниже 54.

Основные операции с конфигурациями осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 13.

Таблица 13. Элементы управления вкладки "Настройки клиентов"

Кнопка	Название	Описание
	Создать	Создание новой конфигурации клиентских компонентов.
	Редактировать	Редактирование выбранной конфигурации.
	Удалить	Удаление выбранных конфигураций.

Перечень полей вкладки приведён в табл. 14.

Таблица 14. Поля вкладки "Настройки клиентов"

Поле	Описание
Имя	Наименование конфигурации клиентских компонентов.
Описание	Описание конфигурации клиентских компонентов.
Созданы	Дата и время создания конфигурации.
Подразделения	Список подразделений, к которым применяется данная конфигурация.

В SoftControl Admin Console представлены следующие категории централизованной настройки клиентских приложений:

- общие настройки 55;
- настройки SoftControl SysWatch 59;
- настройки SoftControl DLP Client 88.

Основные действия, выполняемые с клиентскими конфигурациями:

Создание конфигурации подразделения

Чтобы добавить новую конфигурацию подразделения, нажмите на кнопку **Создать** (рис. Вкладка "Настройки клиентов" 52). В окне **Редактирование настроек клиентов** задайте параметры конфигурации (см. рисунки, начиная с Раздел "Имя и описание" 56 и до Настройки расписания обновления 98). Если внизу окна отображается статус **Значения всех параметров корректны**, нажмите на кнопку **Применить** для добавления созданной конфигурации, в обратном случае измените некорректные значения параметров.

Создание конфигурации подразделения на основе существующей

Чтобы добавить новую конфигурацию на основе уже существующей, выберите её и

выполните одно из следующих действий:

- нажмите на кнопку **Редактировать** в группе кнопок вкладки (рис. Вкладка "Настройки клиентов" 52);
- дважды нажмите левой кнопки мыши на конфигурации.

В окне **Редактирование настроек клиентов** измените имя (обязательно) и параметры конфигурации (в случае необходимости) аналогично работе с новой конфигурацией (см. рисунки, начиная с Раздел "Имя и описание" 56 и до Настройки расписания обновления 98). Если внизу окна отображается статус **Значения всех параметров корректны**, нажмите на кнопку **Применить** для добавления созданной конфигурации, в обратном случае измените некорректные значения параметров.

Изменение типа настроек

Чтобы изменить тип настроек клиентского компонента, перейдите на вкладку Устройства и статусы 39, вызовите контекстное меню требуемого клиентского компонента правой кнопкой мыши и выберите один из пунктов:

- **Использовать настройки подразделения**:
  назначить клиентскому компоненту настройки подразделения, которому он принадлежит.
- **Использовать частные настройки**:
  назначить клиентскому компоненту частные настройки.
- **Отправить повторно настройки клиенту с локальными настройками**:
  назначить клиентскому компоненту SoftControl SysWatch, настройки которого были изменены локально, последнюю конфигурацию, заданную с сервера SoftControl Server.

Использование частных конфигураций

Чтобы добавить новую частную конфигурацию и назначить её клиентскому компоненту, перейдите на вкладку Устройства и статусы 39, вызовите контекстное меню требуемого клиентского компонента правой кнопкой мыши и выберите пункт **Использовать частные настройки**. В окне **Выбор частных настроек** нажмите на кнопку **Добавить** для создания новой частной конфигурации (рис. Управление частными настройками 54).

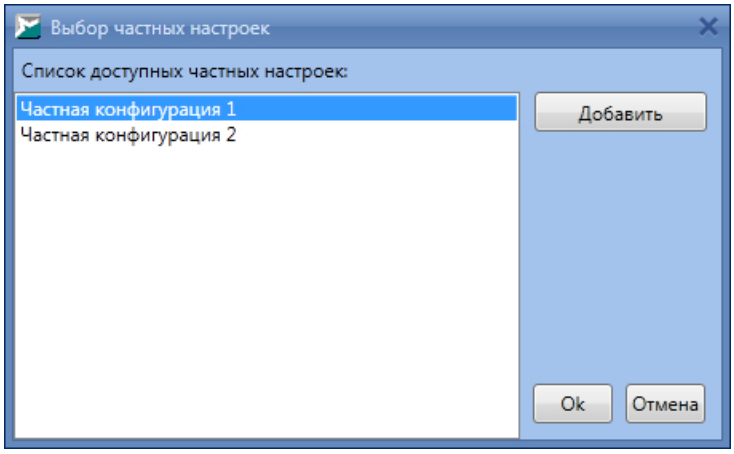


Рисунок 46. Управление частными настройками

В окне **Редактирование настроек клиентов** задайте параметры конфигурации (см. рисунки, начиная с Раздел "Имя и описание" 56 и до Настройки расписания обновления 98). Если внизу окна отображается статус **Значения всех параметров корректны**, нажмите на кнопку **Применить** для добавления созданной конфигурации, в обратном случае измените некорректные значения параметров. Созданная конфигурация будет добавлена в список частных настроек. Выберите в списке её или ранее созданную конфигурацию, после чего нажмите на кнопку **OK** для применения конфигурации к клиентскому компоненту.

Удаление конфигурации

Для удаления конфигурации выберите её, нажмите на кнопку **Удалить** (рис. Вкладка "Настройки клиентов" 52) и подтвердите удаление в диалоговом окне.

4.6.1 Общие настройки

Данная категория настроек включает в себя общие параметры конфигурации и настройки взаимодействия клиентских приложений с сервером.

Имя и описание

Имя конфигурации клиентских приложений необходимо для однозначной идентификации определённого набора настроек, описание конфигурации – для его краткой характеристики.

Чтобы задать **Имя и описание**, в одноимённом разделе категории **Общие**

настройки введите **Имя** и **Описание** в соответствующих полях (рис. Раздел "Имя и описание" 56).

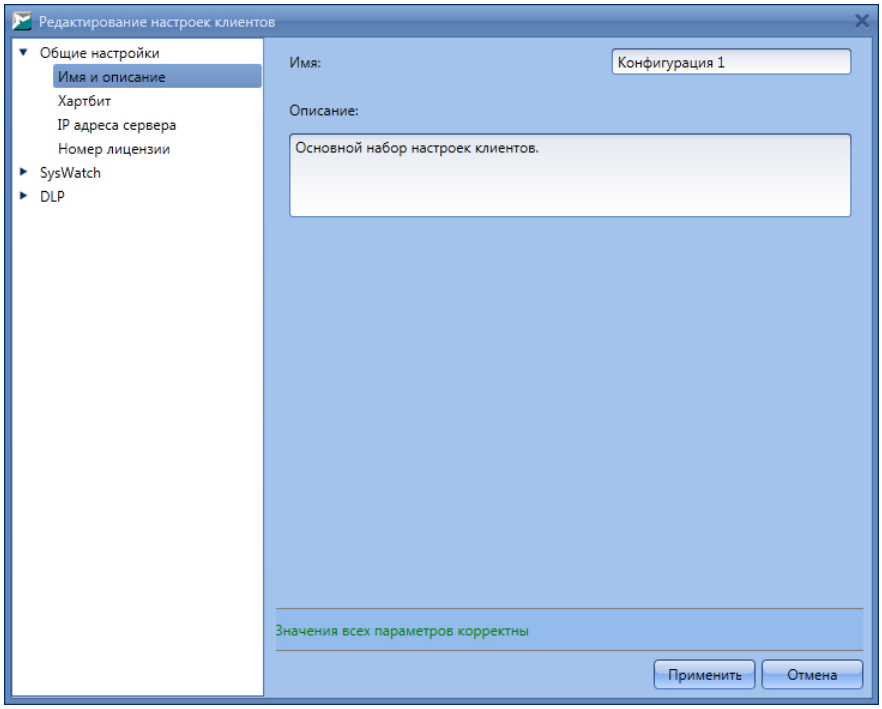


Рисунок 47. Раздел "Имя и описание"

Имя конфигурации должно быть уникальным и не может совпадать с уже существующими конфигурациями.

Хартбит

Хартбит, или интервал обращения клиентского приложения к серверу – параметр клиентских компонентов, отвечающий за периодичность установки связи с серверным компонентом SoftControl Server. По умолчанию устанавливается равным 60 с (1 минута).

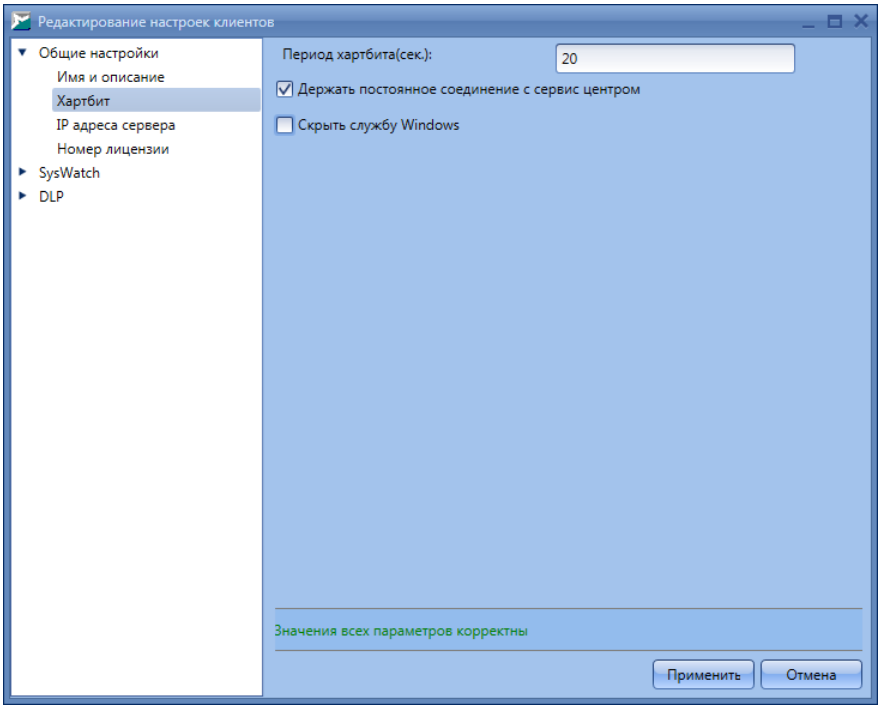


Рисунок 48. Раздел "Хартбит"

Для изменения параметра перейдите в раздел **Хартбит** категории **Общие настройки** и установите значение в поле **Период хартбита (сек.)** (рис. Раздел "Хартбит" 56).

Выставите галочку **Держать постоянное соединение с сервис центром**, если необходимо поддерживать соединение с SoftControl Service Center в режиме реального времени.

Кроме того, галочку **Держать постоянное соединение с сервис центром** следует выставить, если для компонента SoftControl DLP Client необходимо включить запись видео по требованию. Настройки записи видео см. в разделе Настройки SoftControl DLP Client 96.

Выставите галочку **Скрыть службу Windows**, если системные службы SoftControl SysWatch (*safensec.exe*) и SoftControl DLP Client (*eventsvc.exe*) не должны показываться в оснастке **Службы** ОС Windows.

Примечание: скрытие системных служб не работает на ОС Windows XP.

Примечание: если системные службы скрыты, то управление ими средствами ОС становится невозможным.

IP-адреса сервера

Задание адресов сервера для подключения со стороны клиентских приложений

производится мастером настройки сервера[21].

Для изменения списка адресов перейдите в раздел **IP адреса сервера** категории **Общие настройки** (рис. Раздел "IP адреса сервера"[58]). Чтобы добавить адрес в перечень, введите новое значение IP-адреса или NetBIOS-имени в соответствующем поле и нажмите на кнопку **Добавить в список**. Чтобы удалить адрес из перечня, выберите его и нажмите на кнопку **Удалить из списка**.

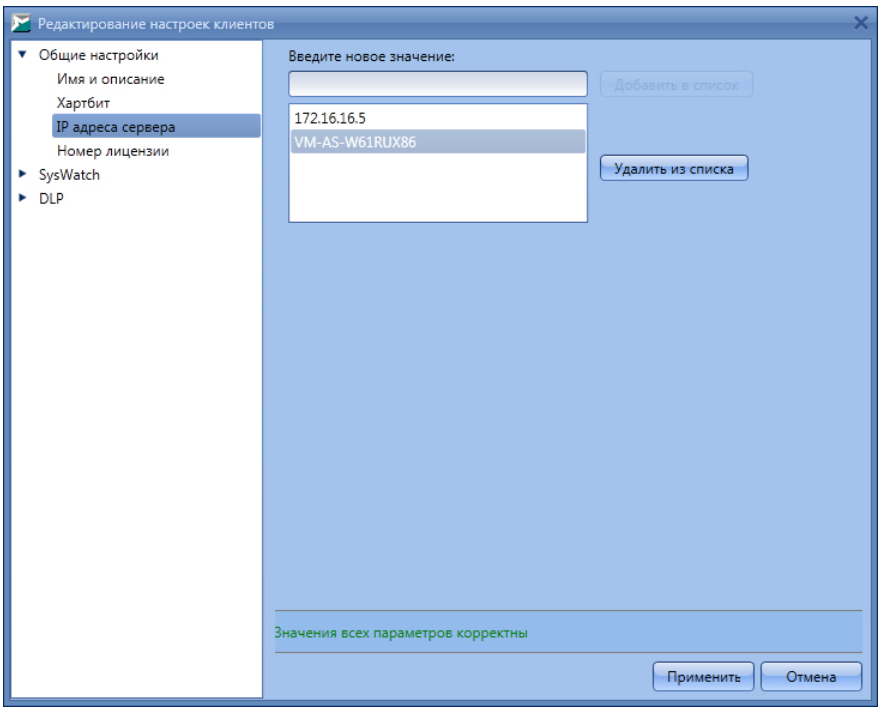


Рисунок 49. Раздел "IP адреса сервера"

Номер лицензии

Лицензионный ключ определяет функциональность клиентских компонентов. По умолчанию устанавливается пробная лицензия сроком действия 30 дней.

Для задания ключа перейдите в раздел **Номер лицензии** категории **Общие настройки**, выберите тип клиентского компонента в выпадающем списке (**SysWatch**, **DLP**), введите ключ в текстовое поле и нажмите на кнопку **Проверить** для валидации лицензии и отображения её параметров в случае корректного ключа (рис. Раздел "Номер лицензии"[58]).

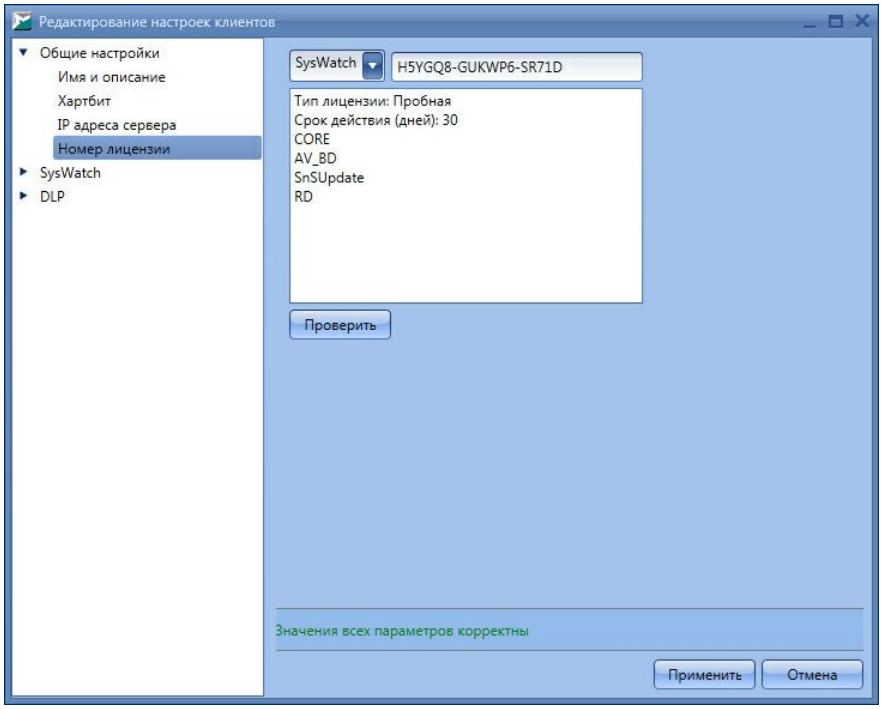


Рисунок 50. Раздел "Номер лицензии"

4.6.2 Настройки SoftControl SysWatch

Данная категория настроек включает в себя конфигурацию клиентского компонента SoftControl SysWatch, аналогичную задаваемой с помощью ГИП SoftControl SysWatch, и политики контроля.

Контроль активности

В разделе **Контроль активности** категории **SysWatch** установите флажки у требуемых областей контроля (рис. Настройки контроля активности 59):

- **Контроль активности**:
  - **Приложения**;
  - **Сеть**;
  - **Файловая система**;
  - **Реестр**.

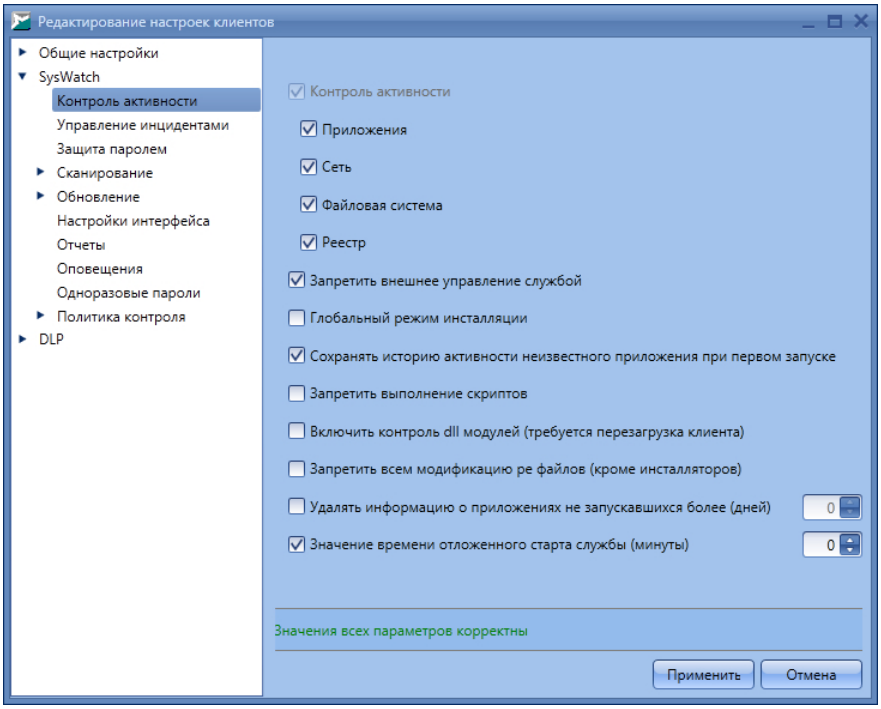


Рисунок 51. Настройки контроля активности

Ниже отметьте необходимые дополнительные опции программы и контроля активности:

- **Запретить внешнее управление службой**:

  запретить выгрузку системной службы SoftControl SysWatch из ОЗУ клиентского хоста.

- **Глобальный режим инсталляции**:

  запускать все процессы в режиме установки.

  При включении данного режима все процессы запускаются с признаком инсталлятора и добавляются в профиль (режим обучения). Кроме того, в профиль добавляются все изменения в исполняемых файлах PE. Рекомендуется использовать только на "чистых" системах, всё ПО для которых устанавливалось с "золотого" образа. Для включения и выключения режима потребуется перезагрузка клиентского хоста.

- **Сохранять историю активности неизвестного приложения при первом запуске**:

  автоматически активировать опцию записи истории активности для новых недоверенных процессов.

- **Запретить выполнение скриптов**:

  заблокировать выполнение недоверенных сценариев интерпретаторами (кроме

сценариев, подписанных действительной ЭЦП или ЭЦП из белого списка сертификатов). Запрещаются следующие процессы:

- wscript.exe (Microsoft ® Windows Based Script Host);
- cscript.exe (Microsoft ® Console Based Script Host);
- java.exe (Java(TM) Platform SE binary);
- javaw.exe (Java(TM) Platform SE binary);
- javaws.exe (Java(TM) Web Start Launcher).

Для запрета запуска определённых процессов рекомендуется создавать соответствующие Правила политики контроля 72.

❑ **Включить контроль dll-модулей**:

активировать контроль целостности динамически подключаемых библиотек (DLL), используемых исполняемыми компонентами.

Контроль запуска dll-модулей работает следующим образом. При попытке загрузить dll-библиотеку SoftControl SysWatch проверяет, подписана ли она ЭЦП. Если библиотека подписана и Windows считает сертификат ЭЦП доверенным, то загрузка библиотеки разрешается (даже если её нет в профиле). Если у библиотеки отсутствует ЭЦП, SoftControl SysWatch проверяет, есть ли данная библиотека в профиле. Если есть, запуск разрешается; если нет – отклоняется.

Примечание: не поддерживается запрет на запуск библиотек, в которых отсутствует точка входа (библиотек, содержащих только ресурсы, без исполняемого кода).

❑ **Запретить всем модификацию ре файлов (кроме инсталляторов)**:

запретить изменение исполняемых файлов недоверенными процессами (не имеющими признака инсталлятора).

Данная функция запрещает любым процессам, которые не признаются доверенными инсталляторами, вносить изменения в dll- или exe-файлы.

❑ **Удалять информацию о приложениях не запускавшихся более (дней)**:

удалять из базы данных SoftControl SysWatch записи о неактивных приложениях, удовлетворяющих заданному условию (число дней без активности).

❑ **Значение времени отложенного старта службы (минуты)**:

установить интервал задержки запуска системной службы SoftControl SysWatch.

Управление инцидентами

В разделе **Управление инцидентами** категории **SysWatch** установите флажок **Включить автоматическую обработку инцидентов** и задайте реакцию на инциденты из перечня **Список инцидентов** в выпадающем списке **Решение** согласно табл. 15 (рис. Настройки реакции на инциденты 62).

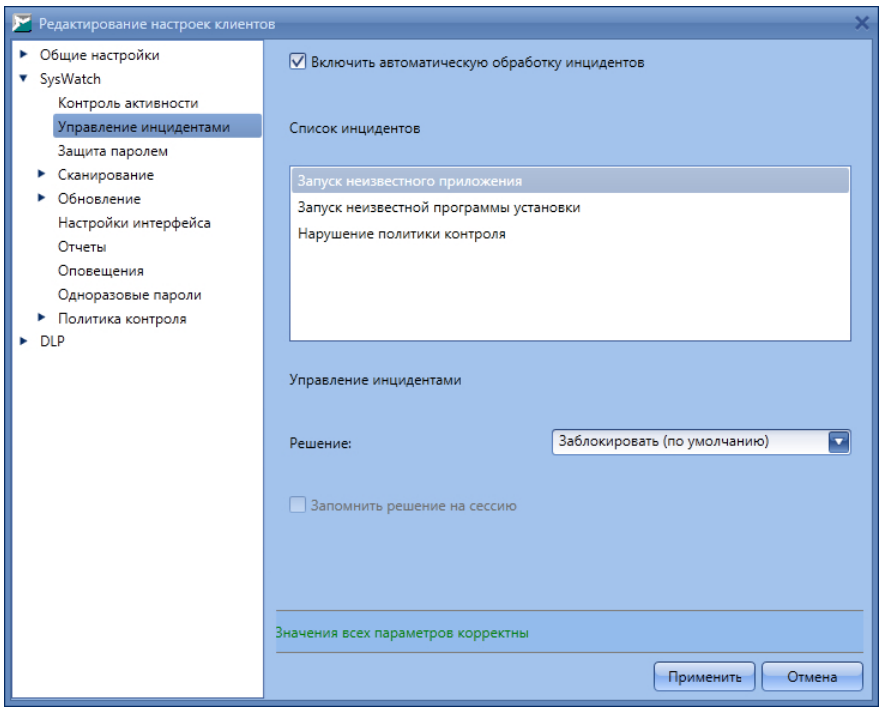


Рисунок 52. Настройки реакции на инциденты

Таблица 15. Возможные действия при инцидентах

Инцидент	Действия
Запуск неизвестного приложения	• **Выполнить в ограниченном режиме** Выполнение приложения под текущей учётной записью либо в изолированной среде ("песочнице") под учётной записью пользователя «V.I.P.O.» с ограниченными правами. При этом добавления в профиль системы не происходит, а приложение помещается в ограниченную зону. Приложение может загружать дочерние модули, которые также не войдут в профиль системы. Даже если такое приложение является вредоносным и выполнит установку каких-либо дополнительных компонентов, то их последующая загрузка будет предотвращена. • **Выполнить в ограниченном режиме после проверки** Запуск приложения в ограниченном режиме, если при антивирусном сканировании приложения не найдено вредоносного кода. В обратном случае запуск будет заблокирован. • **Выполнить в режиме установки** Выполнение приложения под текущей учётной записью без ограничений либо с уменьшенными привилегиями. При этом приложение и все его дочерние модули помещаются в профиль системы и доверенную зону. • **Выполнить в режиме установки после проверки** Запуск приложения в режиме установки, если при антивирусном сканировании

Инцидент	Действия
	приложения не найдено вредоносного кода. В обратном случае запуск будет заблокирован. • **Заблокировать** (по умолчанию) Блокировка запуска приложения и помещение его в запрещённую зону.
Запуск неизвестной программы установки	• **Установить** Выполнение программы установки под текущей учётной записью без ограничений либо с уменьшенными привилегиями. При этом после установки приложение и все его дочерние модули помещаются в профиль системы и доверенную зону. • **Установить после проверки** Запуск установщика в режиме установки, если при антивирусном сканировании установщика не найдено вредоносного кода. В обратном случае запуск будет заблокирован. • **Установить в ограниченном режиме** Выполнение программы установки под текущей учётной записью либо в изолированной среде ("песочнице") под учётной записью пользователя «V.I.P.O.» с ограниченными правами. При этом добавления в профиль системы не происходит, а после установки приложение и все его дочерние модули помещаются в ограниченную зону. • **Установить после проверки в ограниченном режиме** Запуск установщика в ограниченном режиме, если при антивирусном сканировании установщика не найдено вредоносного кода. В обратном случае запуск будет заблокирован. • **Заблокировать** (по умолчанию) Блокировка запуска программы установки и помещение её в запрещённую зону.
Нарушение политики контроля	• **Разрешить** Разрешение процессу выполнить действие, совпадающее с условиями правила заданной политики контроля. • **Разрешить после проверки** Разрешение процессу выполнить действие, совпадающее с условиями правила заданной политики контроля, если при антивирусном сканировании процесса не найдено вредоносного кода. В обратном случае действие будет запрещено. • **Запретить** (по умолчанию) Запрет процессу выполнить действие, совпадающее с условиями правила заданной политики контроля. • **Запретить и завершить приложение** Запрет процессу выполнить действие, совпадающее с условиями правила заданной политики контроля, и последующее завершение процесса. При установке флажка **Запомнить решение на сессию** указанные действия будут выполняться многократно в рамках сессии, в обратном случае – однократно.

Сбросьте флажок **Включить автоматическую обработку инцидентов**, если предполагается делегировать полномочия по обработке инцидентов локальному пользователю SoftControl SysWatch.

Защита паролем

Чтобы установить общий парольный доступ к интерфейсу и/или деинсталлятору SoftControl SysWatch на клиентском хосте, перейдите в раздел **Защита паролем** категории **SysWatch** и установите флажок **Включить защиту паролем** (рис. Настройки парольной защиты 64).

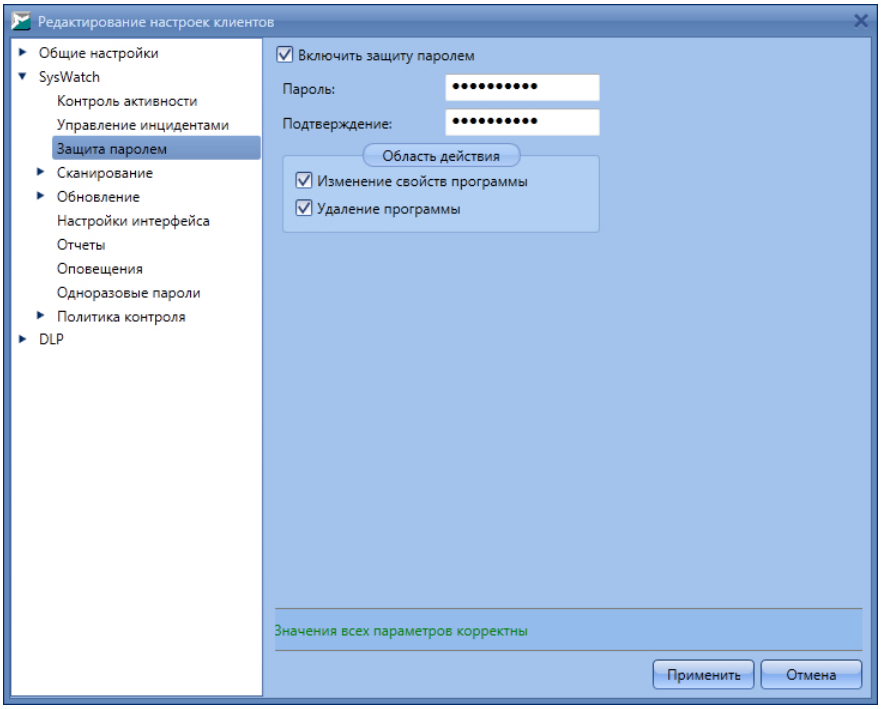


Рисунок 53. Настройки парольной защиты

Задайте **Пароль** и введите его **Подтверждение**, после чего отметьте области действия:

- **Изменение свойств программы**:

  запрос пароля при доступе к ГИП SoftControl SysWatch.

- **Удаление программы**:

  запрос пароля при запуске удаления SoftControl SysWatch.

Настройки сканирования

В разделе **Сканирование** → **Общие настройки** категории **SysWatch** настройте опции антивирусной проверки (рис. Общие настройки сканирования 64).

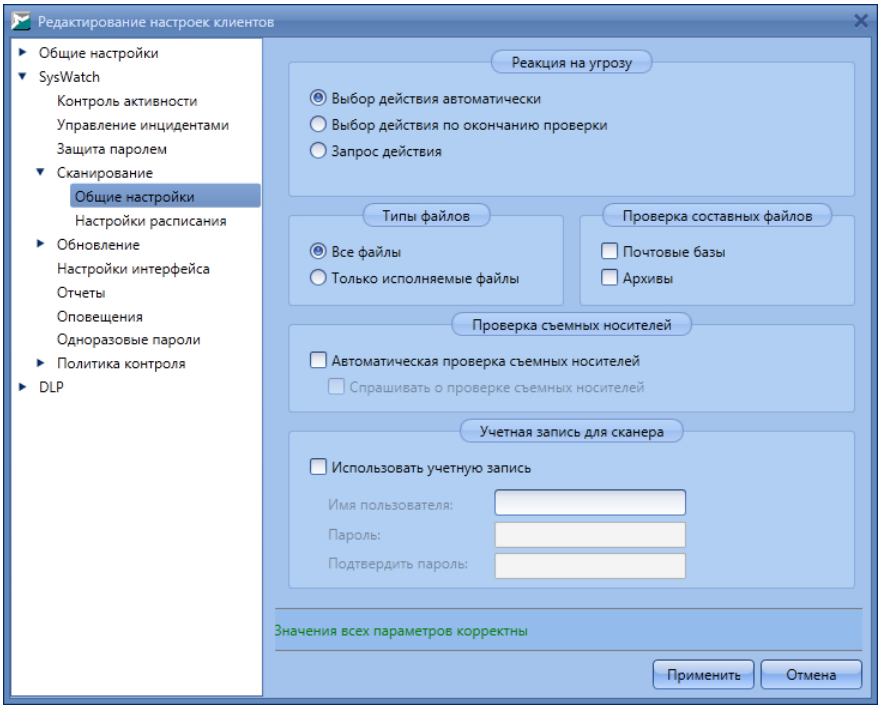


Рисунок 54. Общие настройки сканирования

В области **Реакция на угрозу** выберите один из вариантов действий при обнаружении угроз в процессе антивирусного сканирования:

- **Выбор действия автоматически**:

  Обезвредить инфицированный объект или удалить его, если лечение не удаётся.

- **Выбор действия по окончанию проверки**:

  Запрос действия будет выведен локальному пользователю SoftControl SysWatch по всем обнаруженным угрозам по завершению проверки.

- **Запрос действия**:

  Запрос действия будет выведен локальному пользователю SoftControl SysWatch при обнаружении каждой угрозы.

В области **Типы файлов** выберите типы файлов, которые будут подвергнуты проверке:

- **Все файлы**:

  Сканирование всех типов файлов, за исключением составных типов, не отмеченных в области **Проверка составных файлов** (флажки **Почтовые базы** и **Архивы**).

- **Только исполняемые файлы**

  Сканирование только файлов формата PE.

В области **Проверка съемных носителей** установите флажок **Автоматическая проверка съемных носителей**, если необходимо автоматически запускать антивирусное сканирование USB-носителей после их подключения к клиентскому хосту. Установите флажок **Спрашивать о проверке съемных носителей** для отображения диалогового окна с предложением проверки на клиентском хосте.

В области **Учетная запись для сканера** установите флажок **Использовать учетную запись** и введите учётные данные, если требуется указать учётную запись, под которой будет производиться проверка, отличную от системной на клиентском хосте.

В разделе **Сканирование** → **Настройки расписания** категории **SysWatch** возможно установить расписание антивирусной проверки, для этого установите флажок **Задать расписание** и настройте параметры (рис. Настройки расписания сканирования 66).

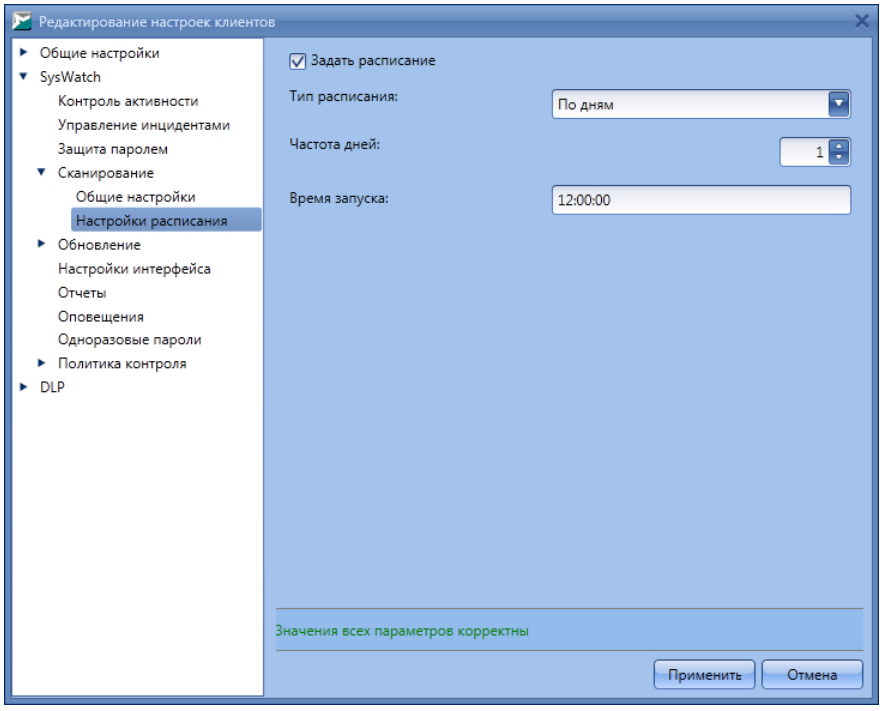


Рисунок 55. Настройки расписания сканирования

В счётчике **Частота дней** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс*.

Настройки обновления

В разделе **Обновление** → **Общие настройки** категории **SysWatch** настройте опции обновления (рис. Общие настройки обновления 67).

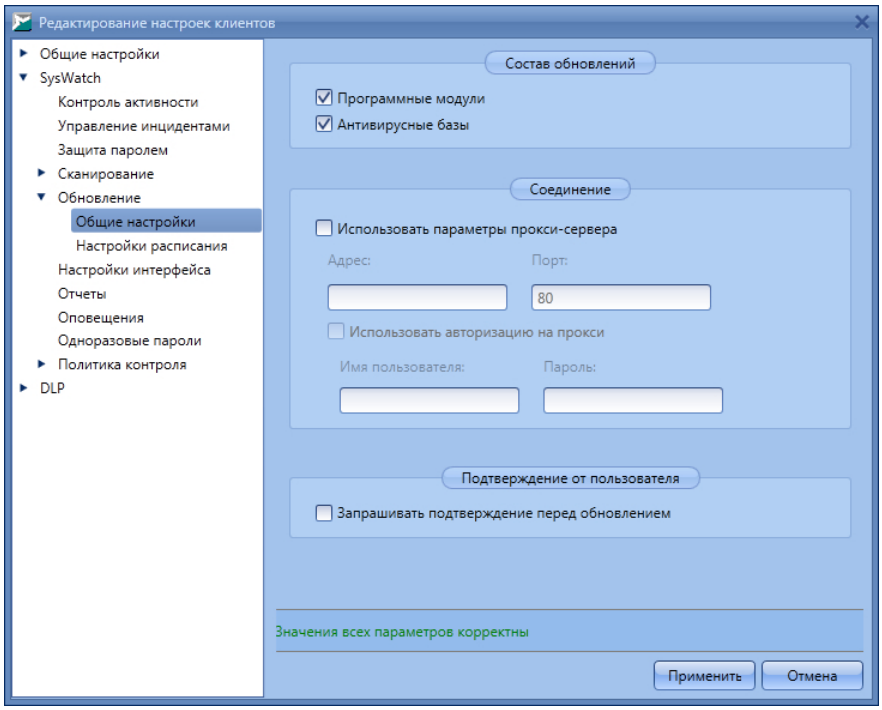


Рисунок 56. Общие настройки обновления

В области **Состав обновлений** выберите требуемые компоненты SoftControl SysWatch для обновления:

- ❑ **Программные модули**;
- ❑ **Антивирусные базы**.

В области **Соединение** установите флажок **Использовать параметры прокси-сервера** и укажите необходимые настройки, если для соединения с интернет-сервером обновлений используется прокси-сервер.

В области **Подтверждение от пользователя** установите флажок **Запрашивать подтверждение перед обновлением**, если требуется отображать диалог с запросом подтверждения операции на клиентском хосте.

В разделе **Обновление** → **Настройки расписания** категории **SysWatch** возможно установить расписание обновления, для этого установите флажок **Задать расписание** и настройте параметры (рис. Настройки расписания обновления 67). В счётчике **Частота дней** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс*.

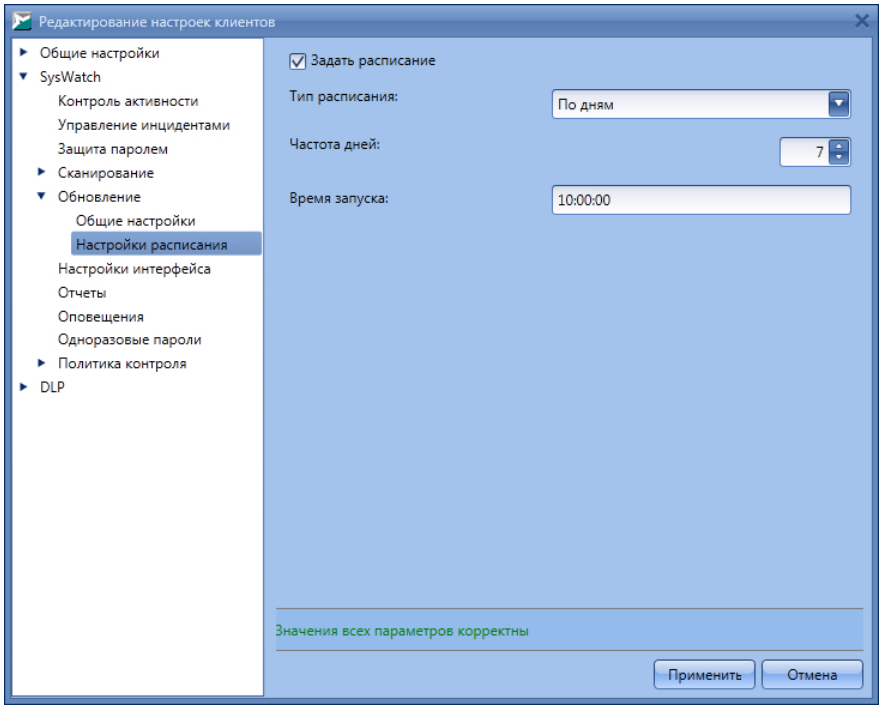


Рисунок 57. Настройки расписания обновления

Одноразовые пароли

В разделе **Одноразовые пароли** категории **SysWatch** установите флажок **Включить одноразовые пароли** и нажмите на кнопку (**Сгенерировать ключ**) для выработки 256-битного ключа, на основе которого будут вычисляться одноразовые пароли (рис. Настройки одноразовых паролей 68).

Смена ключа делает недействительными все предыдущие пароли.

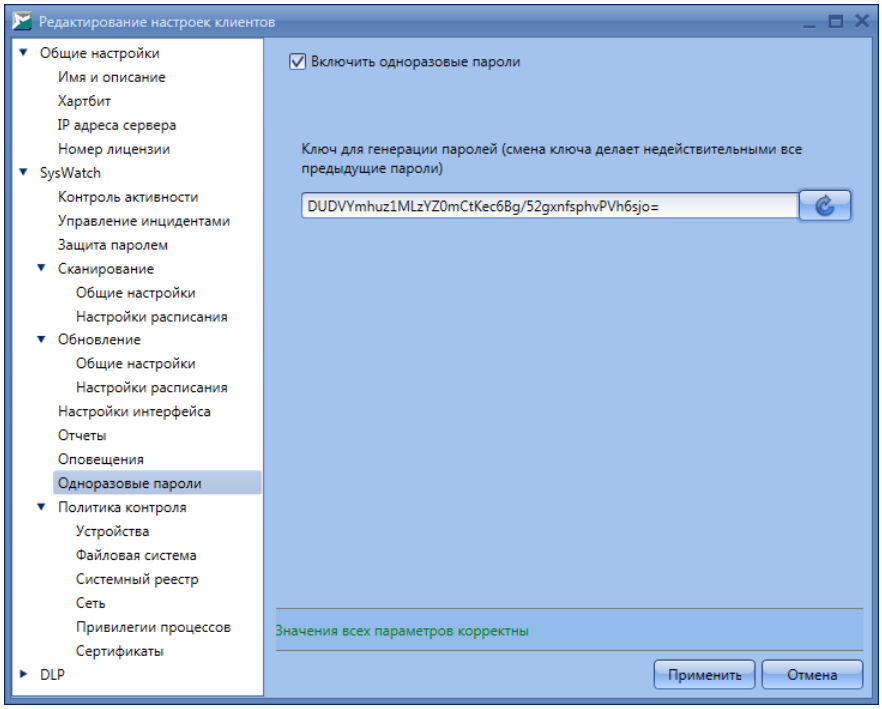


Рисунок 58. Настройки одноразовых паролей

Непосредственная генерация одноразовых паролей осуществляется на вкладке Подразделения 50.

Отчеты

В разделе **Отчеты** категории **SysWatch** настройте параметры SoftControl SysWatch по протоколированию в текстовые отчёты и регистрации событий в WMI (рис. Настройки отчётов 69).

В области **Отчеты** установите флажок **Формировать отчеты**, чтобы включить функцию ведения текстовых отчётов, и выберите виды событий для протоколирования:

- **Обновление**;
- **Проверка**;
- **Системный**:
  - **Угрозы**;
  - **Доверенные процессы**.

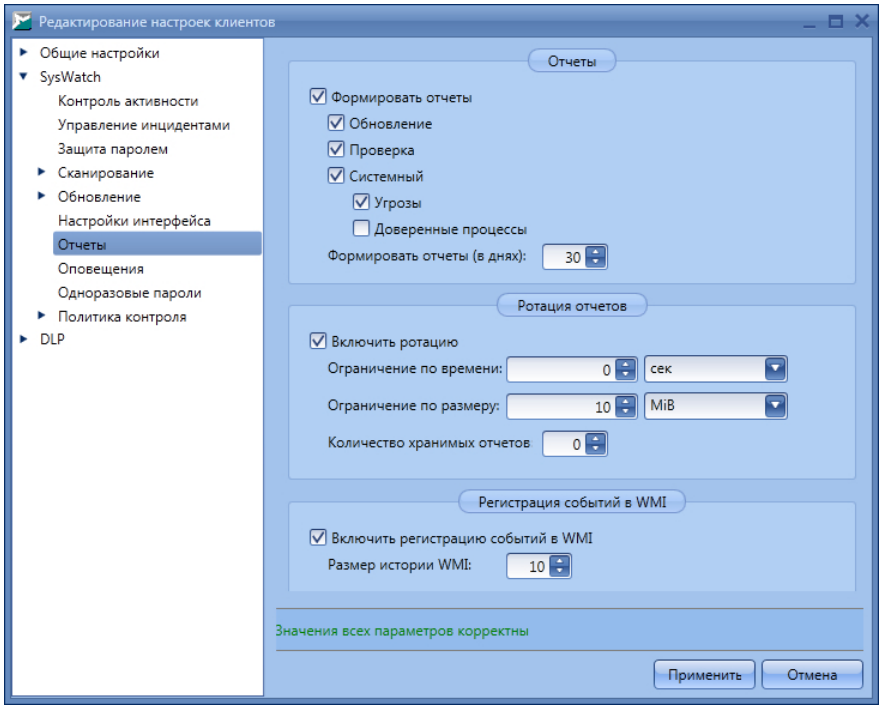


Рисунок 59. Настройки отчётов

Выставите галочку **Доверенные процессы**, чтобы включить запись событий запуска/останова служб. Службы, которые были запущены до системной службы *safensec.exe*, будут помечаться в отчётах как *была запущена ранее*.

В счётчике **Формировать отчеты (в днях)** установите количество дней, за которые сохраняется история событий.

В области **Ротация отчётов** при необходимости установите флажок **Включить ротацию** и укажите параметры ротации (один или несколько), ограничивающие количественные характеристики текстовых отчётов:

- **Ограничение по времени**:

  введите в данном поле временной лимит одного файла отчёта и выберите единицы величины в выпадающем списке (секунды, минуты, часы, дни).

- **Ограничение по размеру**:

  введите в данном поле лимит по размеру одного файла отчёта и выберите единицы величины в выпадающем списке (Б, КиБ, МиБ).

- **Количество хранимых логов**:

  введите в данном поле максимальное число хранимых частей файлов отчётов.

В области **Регистрация событий в WMI** установите флажок **Включить регистрацию событий в WMI** для включения соответствующей функции и укажите

Размер истории WMI в одноименном поле.

> Для предотвращения проблем с повышенным потреблением системных ресурсов не рекомендуется задавать размер истории равным более 100 событий, оптимальная величина – от 10 до 50 событий.

Настройки интерфейса

В разделе **Настройки интерфейса** категории **SysWatch** выберите необходимые опции интерфейса SoftControl SysWatch на клиентских хостах (рис. Настройки интерфейса 71):

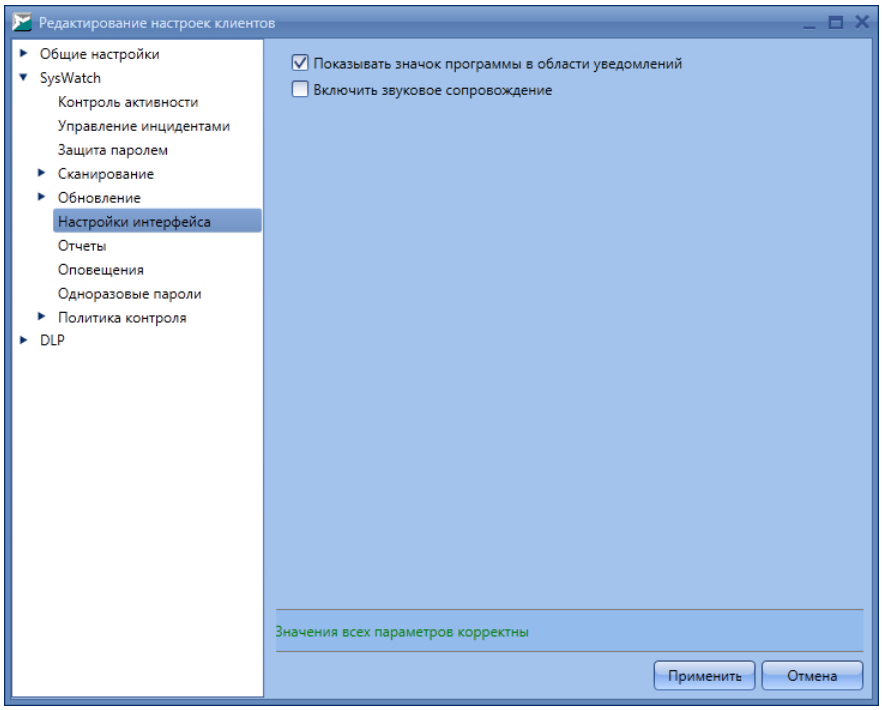


Рисунок 60. Настройки интерфейса

- **Показывать значок программы в области уведомлений**: отображение значка SoftControl SysWatch в области уведомлений.
- **Включить звуковое сопровождение**: сопровождать уведомления программы звуками.

Оповещения

В разделе **Оповещения** категории **SysWatch** установите флажок **Показывать оповещения** для отображения локальных оповещений SoftControl SysWatch на клиентских хостах и выберите необходимые типы сообщений (рис. Настройка локальных оповещений 72):

- **Статус защиты**;
- **Обновление программы**;
- **Проверка компьютера**;
- **Отчеты**;
- **Лицензия**;
- **Установка (удаление) программ**;
- **Блокирование модулей программы**;
- **Ограничение приложений**.

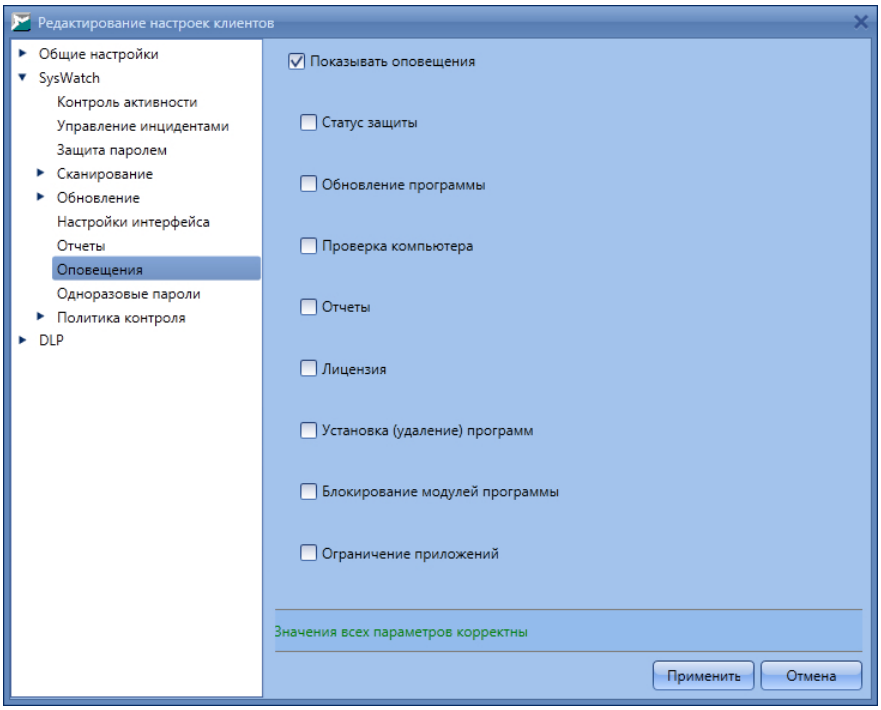


Рисунок 61. Настройка локальных оповещений

Политика контроля: Файловая система

В разделе **Политика контроля** → **Файловая система** категории **SysWatch** определите правила доступа приложений к объектам файловой системы на клиентских хостах (рис. Политика контроля файловой системы 72):

- Чтение файла или каталога;
- Запись в файл или каталог (создание/изменение файла или каталога);
- Удаление файла или каталога.

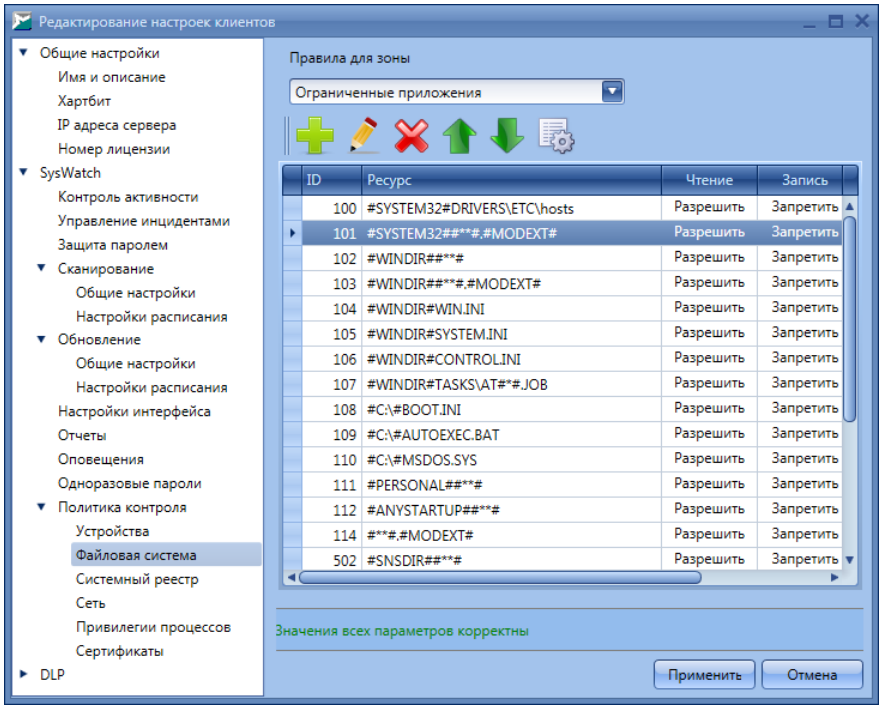


Рисунок 62. Политика контроля файловой системы

Правила разделены по спискам для приложений из следующих зон выполнения:

- **Доверенные приложения**;
- **Ограниченные приложения**.

Для переключения между списками выберите соответствующую категорию в выпадающем списке **Правила для зоны**. Если требуется переместить правило в список для приложений из другой зоны выполнения, вызовите контекстное меню правила и выберите один из вариантов:

- **Все** – создать правило для обеих зон выполнения, если правило находится только в одном списке;
- **Ограниченные** – переместить правило в список правил для ограниченных приложений;
- **Доверенные** – переместить правило в список правил для доверенных приложений.

Каждое правило представляет собой запись в линейном списке и имеет свой уникальный идентификатор **ID**. Объекты применения указываются в столбце **Ресурс**, права доступа к ним – в столбцах **Чтение**, **Запись** и **Удаление**. Флажок в столбце **Активно** указывает действует ли данное правило.

Если несколько правил имеют пересекающиеся области действия, то приоритет

выполнения в таком случае имеет правило, расположенное в списке наиболее низко. Положение правила в списке изменяется с помощью кнопок (**Вверх**) и (**Вниз**).

Строка в столбце **Ресурс** представляет собой путь до объекта или объектов применения правила. В данной строке могут использоваться маски – инструмент задания правил для группы объектов файловой системы. Например, с помощью масок можно создать правило для каталога и всех объектов внутри него или правило для определённых типов (расширений) файлов.

Ниже приведён синтаксис масок:

- **#*#** – заменяет любое количество символов, кроме символа '\' (в случае размещения в конце строки распространяется только на файлы корневой директории);
- **#**#** – заменяет любое количество символов (в случае размещения в конце строки распространяется на файлы корневой директории, поддиректории и файлы поддиректорий);
- **#?#** – заменяет ровно 1 любой символ.

Чтобы создать правило, нажмите на кнопку (**Добавить**).

В появившемся окне введите полный путь до объекта файловой системы или маску в поле **Файл или каталог** (рис. Создание правила для объекта файловой системы 74).

Вы можете указывать как папки на локальном жёстком диске, так и сетевые папки.

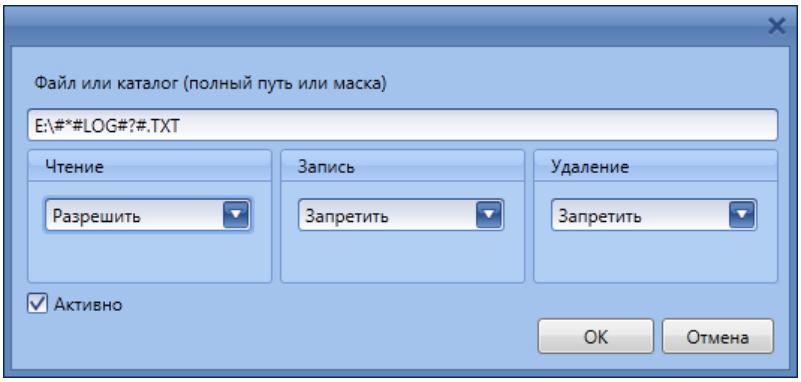


Рисунок 63. Создание правила для объекта файловой системы

В областях **Чтение**, **Запись** и **Удаление** выберите в выпадающих списках соответствующие права доступа к объекту:

- **Разрешить** – позволить приложению выполнять операцию над объектом;
- **Запретить** – заблокировать выполнение приложением операции над объектом;
- **Запрос** – выводить запрос при совпадении действия над объектом с условием

правила.

Чтобы включить созданное правило в список и сделать его действующим, установите флажок **Активно** и нажмите на кнопку **OK**.

Чтобы изменить правило, нажмите на кнопку (**Изменить**) или дважды нажмите на него и настройте параметры правила аналогично действиям при его создании.

Чтобы задать время действия правила и пользователей, к которым оно применяется, нажмите на кнопку (**Дополнительно**). В появившемся окне укажите временные интервалы и добавьте пользователей с помощью кнопки **Добавить** (рис Добавление временных интервалов и пользователей для правила 75). Чтобы изменения вступили в силу, нажмите на кнопку **Применить**.

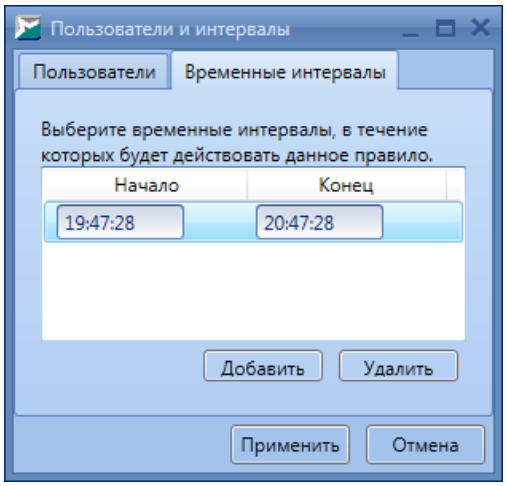


Рисунок 64. Добавление временных интервалов и пользователей для правила

Чтобы удалить правило, нажмите на кнопку (**Удалить**).

> В наборе политик контроля SoftControl SysWatch содержатся предустановленные правила, распространяющиеся на системные каталоги и объекты расположения компонентов продукта. Изменение или удаление предустановленных правил может повлечь за собой нарушение защиты целостности системы клиентского хоста.

Политика контроля: Системный реестр

В разделе **Политика контроля** → **Системный реестр** категории **SysWatch** определите правила доступа приложений к объектам системного реестра на клиентских хостах (рис. Политика контроля системного реестра 76):

- Запись в ключ или параметр реестра (создание/изменение ключа или параметра);
- Удаление ключа или параметра реестра.

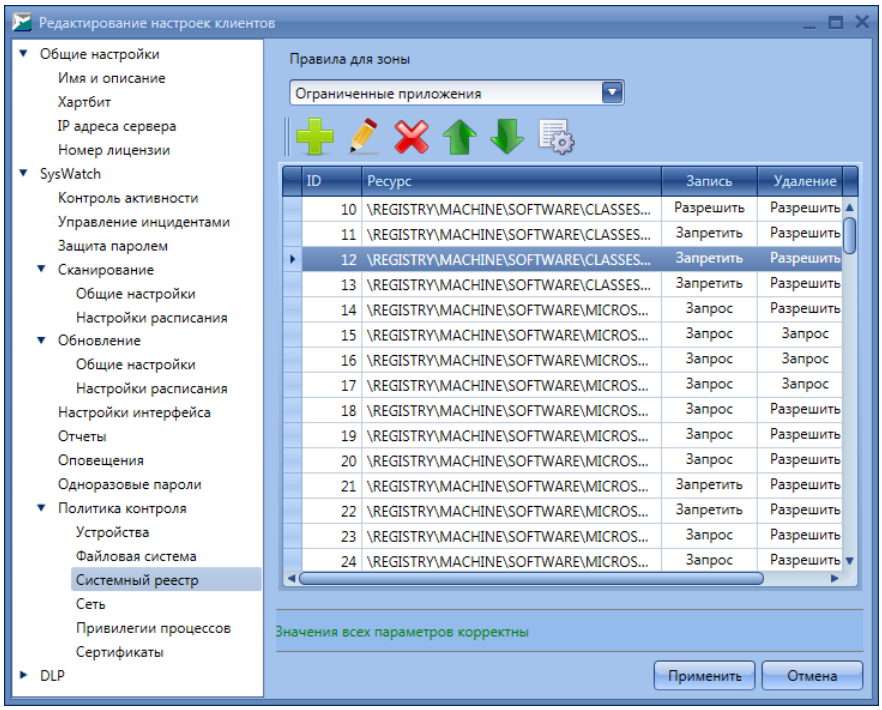


Рисунок 65. Политика контроля системного реестра

Правила разделены по спискам для приложений из следующих зон выполнения:

- **Доверенные приложения**;
- **Ограниченные приложения**.

Для переключения между списками выберите соответствующую категорию в выпадающем списке **Правила для зоны**. Если требуется переместить правило в список для приложений из другой зоны выполнения, вызовите контекстное меню правила и выберите один из вариантов:

- **Все** – создать правило для обеих зон выполнения, если правило находится только в одном списке;
- **Ограниченные** – переместить правило в список правил для ограниченных приложений;
- **Доверенные** – переместить правило в список правил для доверенных приложений.

Каждое правило представляет собой запись в линейном списке и имеет свой уникальный идентификатор **ID**. Объекты применения указываются в столбце **Ресурс**, права доступа к ним – в столбцах **Запись** и **Удаление**. Флажок в столбце **Активно**

указывает действует ли данное правило.

Если несколько правил имеют пересекающиеся области действия, то приоритет выполнения в таком случае имеет правило, расположенное в списке наиболее низко. Положение правила в списке изменяется с помощью кнопок (**Вверх**) и (**Вниз**).

Строка в столбце **Ресурс** представляет собой путь до объекта или объектов применения правила. В данной строке могут использоваться маски – инструмент задания правил для группы объектов системного реестра. Например, с помощью масок можно создать правило для раздела реестра и всех объектов внутри него.

Ниже приведён синтаксис масок:

- **#*#** – заменяет любое количество символов, кроме символа '\' (в случае размещения в конце строки распространяется только на параметры раздела);
- **#**#** – заменяет любое количество символов (в случае размещения в конце строки распространяется на параметры раздела, подразделы и параметры подразделов);
- **#?#** – заменяет ровно 1 любой символ.

Чтобы создать правило, нажмите на кнопку (**Добавить**).

В появившемся окне введите полный путь до объекта системного реестра или маску в поле **Ключ или параметр реестра**, (рис. Создание правила для объекта системного реестра 77), при этом корневые разделы реестра в задаваемом пути должны быть указаны следующим образом:

- *\REGISTRY\MACHINE\SOFTWARE\CLASSES* – раздел HKEY_CLASSES_ROOT;
- *\REGISTRY\MACHINE* – раздел HKEY_LOCAL_MACHINE;
- *\REGISTRY\USER\<SID>* – раздел HKEY_CURRENT_USER для пользователя с указанным идентификатором безопасности (<SID>);
- *\REGISTRY\USER* – раздел HKEY_USERS.

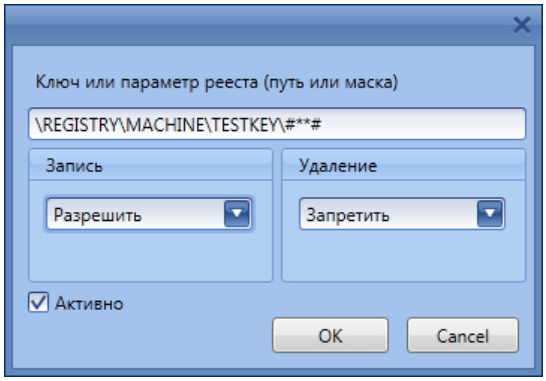


Рисунок 66. Создание правила для объекта системного реестра

В областях **Запись** и **Удаление** выберите в выпадающих списках соответствующие права доступа к объекту:

- **Разрешить** – позволить приложению выполнять операцию над объектом;
- **Запретить** – заблокировать выполнение приложением операции над объектом;
- **Запрос** – выводить запрос при совпадении действия над объектом с условием правила.

Чтобы включить созданное правило в список и сделать его действующим, установите флажок **Активно** и нажмите на кнопку **OK**.

Чтобы изменить правило, нажмите на кнопку (**Изменить**) или дважды нажмите на него и настройте параметры правила аналогично действиям при его создании.

Чтобы задать время действия правила и пользователей, к которым оно применяется, нажмите на кнопку (**Дополнительно**). В появившемся окне укажите временные интервалы и добавьте пользователей с помощью кнопки **Добавить** (рис Добавление временных интервалов и пользователей для правила 78). Чтобы изменения вступили в силу, нажмите на кнопку **Применить**.

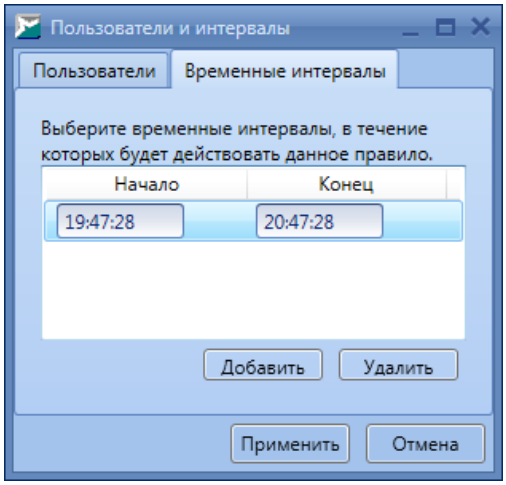


Рисунок 67. Добавление временных интервалов и пользователей для правила

Чтобы удалить правило, нажмите на кнопку ✖ (**Удалить**).

В наборе политик контроля SoftControl SysWatch содержатся предустановленные правила, распространяющиеся на ключи и параметры реестра, влияющие на работу системы и компонентов продукта. Изменение или удаление предустановленных правил может повлечь за собой нарушение защиты целостности системы клиентского хоста.

Политика контроля: Устройства

В разделе **Политика контроля** → **Устройства** категории **SysWatch** настройте правила использования следующих внешних устройств и портов системы на клиентских хостах (рис. Политика контроля устройств 79):

- USB-устройства;
- CD/DVD-устройства;
- LPT-порты;
- COM-порты.

Чтобы определить права доступа к USB-устройствам, задайте их соответствующими флажками в столбцах **Чтение**, **Запись** и **Удаление** для типа **USB устройства**.

Дополнительно можно задать исключения – белый список USB-устройств, для которых назначенное правило действовать не будет. Для этого нажмите на ссылку **Дополнительно** и в появившемся окне нажмите на кнопку ✚ (**Добавить**) (рис. Исключения для USB-устройств 80).

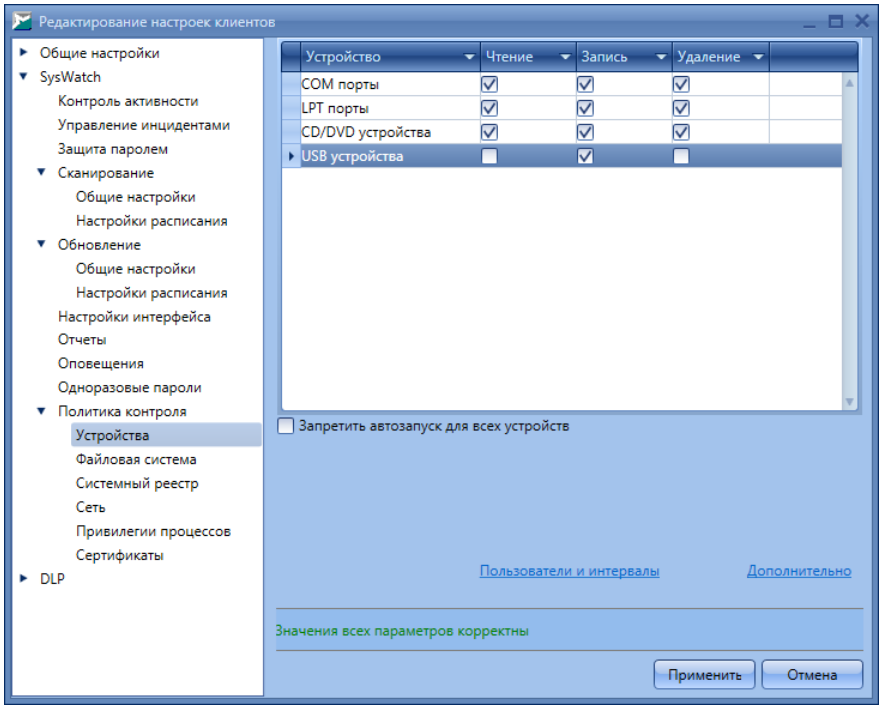


Рисунок 68. Политика контроля устройств

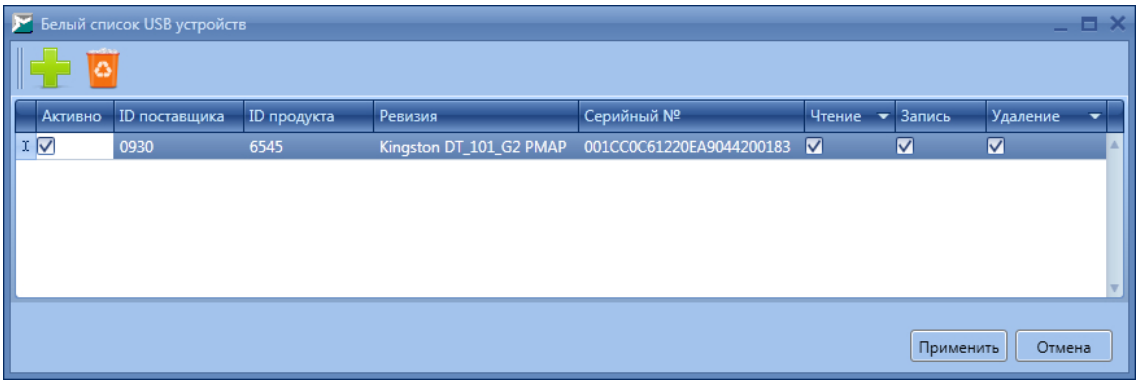


Рисунок 69. Исключения для USB-устройств

Введите параметры USB-устройства в соответствующих полях. Получить данные параметры USB-устройства можно следующим образом:

1) Вставьте носитель в USB-порт компьютера.
2) Откройте оснастку **Диспетчер устройств** (Device Manager) Панели управления Windows.
3) Разверните категорию **Дисковые устройства** (Disk drives) и дважды нажмите левой кнопкой мыши на имени искомого USB-носителя.
4) В появившемся окне перейдите на вкладку **Сведения** (Details).
5) В выпадающем меню выберите свойство **Родитель** (Parent). В поле **Значение** (Value) отобразится строка вида:

USB\VID_<ID поставщика>&PID_<ID продукта>\<Серийный №>,

где указаны соответствующие числовые значения параметров **ID поставщика**, **ID продукта** и **Серийный №** (показаны в угловых скобках).

6) В выпадающем меню выберите свойство **ИД оборудования** (Hardware Ids). В поле **Значение** (Value) отобразится список аппаратных идентификаторов, первый из которых необходимо использовать в качестве параметра **Ревизия**.

После ввода параметров выберите права доступа для данного устройства в соответствующих столбцах **Чтение**, **Запись** и **Удаление**. Чтобы включить устройство в белый список, установите флажок в столбце **Активно**.

Чтобы удалить устройство из списка, нажмите на кнопку (**Удалить**).

Правила сохраняются после нажатия на кнопку **Применить**.

Для USB-устройств можно также задать временные интервалы и пользователей, для которых будут действовать выбранные права доступа. Для этого нажмите на ссылку **Пользователи и интервалы**. В появившемся окне укажите временные интервалы и добавьте пользователей с помощью кнопки **Добавить** (рис Добавление временных интервалов и пользователей для правила 81). Чтобы изменения вступили в силу, нажмите на кнопку **Применить**.

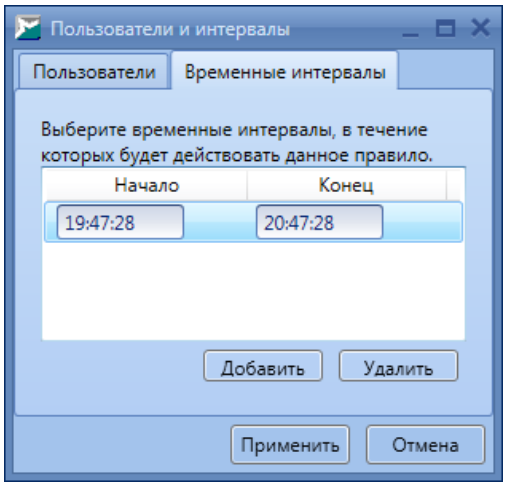


Рисунок 70. Добавление временных интервалов и пользователей для правила

Чтобы заблокировать доступ к CD/DVD-устройствам, COM-портам или LPT-портам, сбросьте любой из флажков в столбцах **Чтение**, **Запись** или **Удаление** для соответствующих типов устройств (при этом будут сброшены все флажки для данного типа).

Для изменения прав доступа к портам (COM, LPT) дополнительно необходима перезагрузка системы на клиентских хостах.

Отметьте опцию **Запретить автозапуск для всех устройств**, если требуется блокировать автозагрузку всех USB- и CD/DVD-устройств.

Политика контроля: Сеть

В разделе **Политика контроля** → **Сеть** категории **SysWatch** определите правила контроля сетевой активности приложений на клиентских хостах (рис. Политика контроля сетевой активности 82):

- Приём данных;
- Передача данных.

Правила разделены по спискам для приложений из следующих зон выполнения:

- **Доверенные приложения**;
- **Ограниченные приложения**.

Для переключения между списками выберите соответствующую категорию в выпадающем списке **Правила для зоны**. Если требуется переместить правило в список для приложений из другой зоны выполнения, вызовите контекстное меню правила и выберите один из вариантов:

- **Все** – создать правило для обеих зон выполнения, если правило находится только в одном списке;
- **Ограниченные** – переместить правило в список правил для ограниченных приложений;
- **Доверенные** – переместить правило в список правил для доверенных приложений.

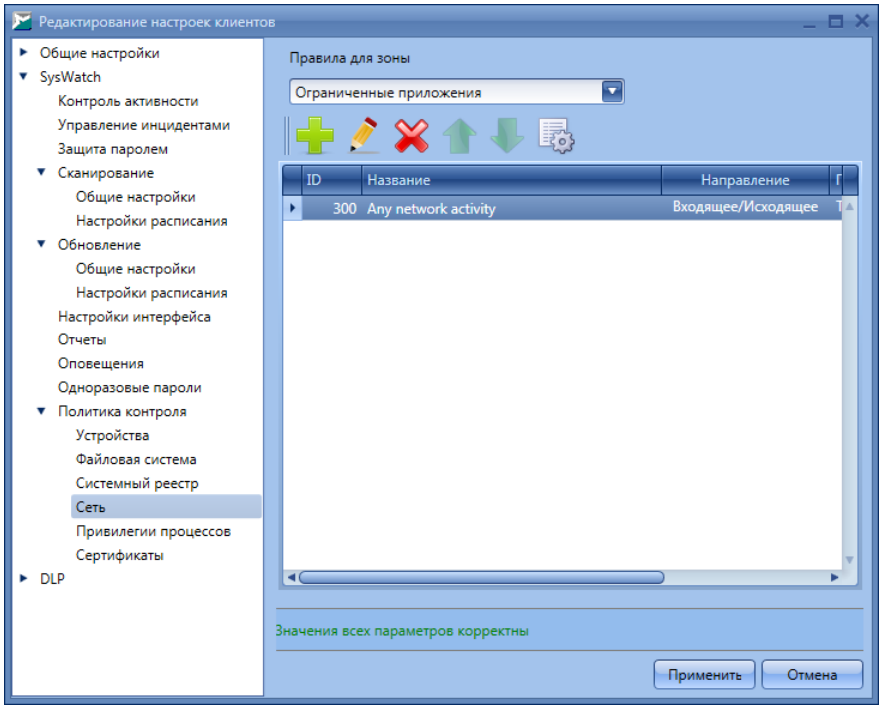


Рисунок 71. Политика контроля сетевой активности

Каждое правило представляет собой запись в линейном списке и имеет свой уникальный идентификатор **ID**. Параметры правила указаны в столбцах **Название**, **Направление** и **Протокол**. Разрешение или запрет сетевого соединения индицируется флажком в столбце **Разрешение**, необходимость обработки события, в случае его наступления, локальным пользователем – в столбце **Подтверждение**. Флажок в столбце **Активно** указывает действует ли данное правило.

Если несколько правил имеют пересекающиеся области действия, то приоритет выполнения в таком случае имеет правило, расположенное в списке наиболее низко. Положение правила в списке изменяется с помощью кнопок (**Вверх**) и (**Вниз**).

Чтобы создать правило, нажмите на кнопку (**Добавить**).

В появившемся окне задайте параметры правила (рис. Создание правила контроля сетевой активности 84):

- **Название** – наименование правила.
- **Направление** – направление сетевой активности, определяющее инициатора соединения:
  - **Входящее** – сетевое соединение, инициируемое удалённым хостом;
  - **Исходящее** – сетевое соединение, инициируемое клиентским хостом;
  - **Входящее/Исходящее** – любое из направлений.

- **Протокол** – тип протокола передачи данных по сети:
  - **TCP**;
  - **UDP**;
  - **TCP/UDP** – любой из протоколов.

На вкладках **Локальный адрес** и **Удаленный адрес** задаются конечные точки, между которыми осуществляется передача данных, на клиентском и удалённом хостах соответственно. В обеих вкладках выберите на какие сетевые адреса и порты распространяется действие правила и введите значения в соответствующие поля при необходимости:

- **Адрес** – IP-адрес узла сети:
  - **Любой адрес**;
  - **Определенный адрес**;
  - **Диапазон адресов**.
- **Порт** – сетевой порт:
  - **Любой порт**;
  - **Определенный порт**;
  - **Диапазон портов**.

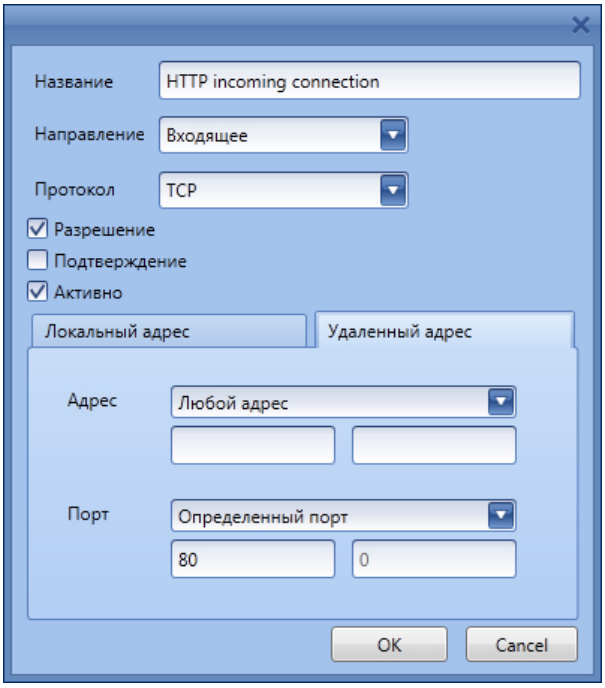


Рисунок 72. Создание правила контроля сетевой активности

Для разрешения сетевого соединения с указанными параметрами установите

флажок **Разрешение**, для запрещения – сбросьте его. Если предполагается обработка событий сетевой активности приложений локальным пользователем на клиентском хосте, установите флажок **Подтверждение** (при этом должна быть отключена автоматическая обработка инцидентов [61]).

Чтобы включить созданное правило в список и сделать его действующим, установите флажок **Активно** и нажмите на кнопку **OK**.

Чтобы изменить правило, нажмите на кнопку (**Изменить**) или дважды нажмите на него и настройте параметры правила аналогично действиям при его создании.

Чтобы задать время действия правила и пользователей, к которым оно применяется, нажмите на кнопку (**Дополнительно**). В появившемся окне укажите временные интервалы и добавьте пользователей с помощью кнопки **Добавить** (рис Добавление временных интервалов и пользователей для правила [85]). Чтобы изменения вступили в силу, нажмите на кнопку **Применить**.

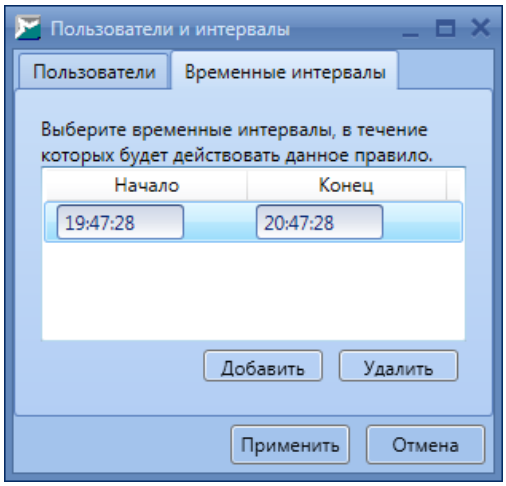


Рисунок 73. Добавление временных интервалов и пользователей для правила

Чтобы удалить правило, нажмите на кнопку (**Удалить**).

Политика контроля: Привилегии процессов

В разделе **Политика контроля** → **Привилегии процессов** категории **SysWatch** настройте ограничения на использование процессами следующих привилегий Windows на клиентских хостах (рис. Политика контроля привилегий процессов [86]):

- Архивация файлов и каталогов;
- Обход перекрестной проверки;
- Создание глобальных объектов;

- Создание файла подкачки;
- Отладка программ;
- Имитация клиента после проверки пользователя;
- Увеличение приоритета выполнения;
- Настройка квот памяти для процесса;
- Загрузка и выгрузка драйверов устройств;
- Выполнение задач по обслуживанию томов;
- Профилирование одного процесса;
- Принудительное удалённое завершение работы;
- Восстановление файлов и каталогов;
- Управление аудитом и журналом безопасности;
- Завершение работы системы;
- Изменение параметров среды изготовителя;
- Профилирование производительности системы;
- Изменение системного времени;
- Смена владельцев файлов и других объектов;
- Отключение компьютера от стыковочного узла.

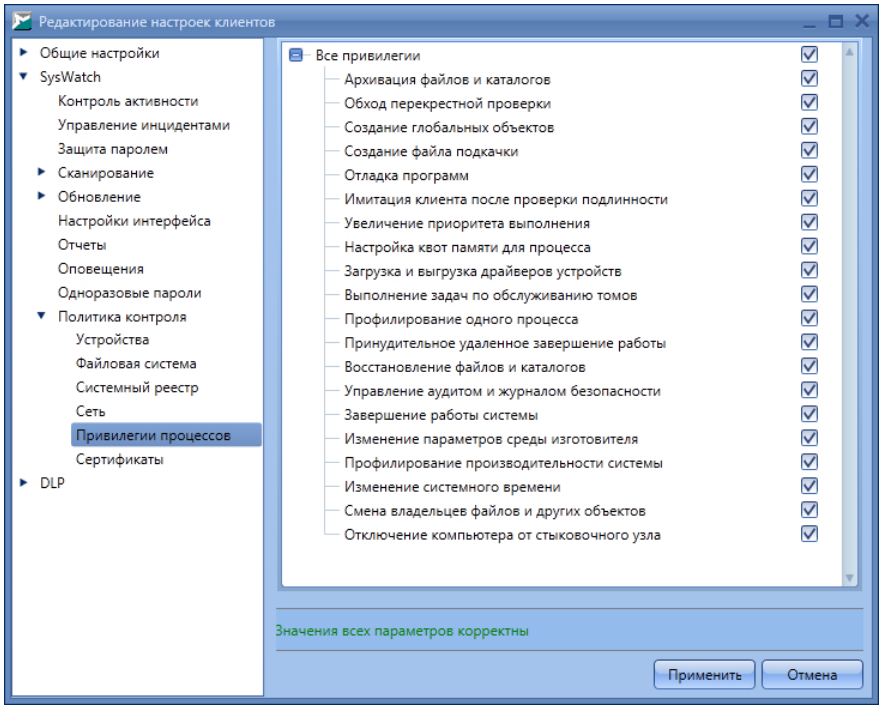


Рисунок 74. Политика контроля привилегий процессов

Условие: правила распространяются на все приложения из ограниченной зоны

выполнения.

По умолчанию, приложения (процессы) обладают всеми вышеуказанными привилегиями, но при этом могут быть ограничены ОС. Чтобы ограничить привилегии вручную, сбросьте флажки у требуемых привилегий.

Политика контроля: Сертификаты

В разделе **Политика контроля** → **Сертификаты** категории **SysWatch** определите белый список сертификатов ЭЦП для дополнительного контроля активности процессов на клиентских хостах (рис. Белый список сертификатов 87).

При запуске процесса SoftControl SysWatch эвристически определяет является ли он программой установки или сценарием. По умолчанию, в этом случае процесс получает признак инсталлятора, если имеет действительную ЭЦП. Помимо этого, возможна дополнительная проверка сертификата ЭЦП на наличие в белом списке сертификатов. Для этого установите флажок **Использовать белый список сертификатов** и сформируйте список.

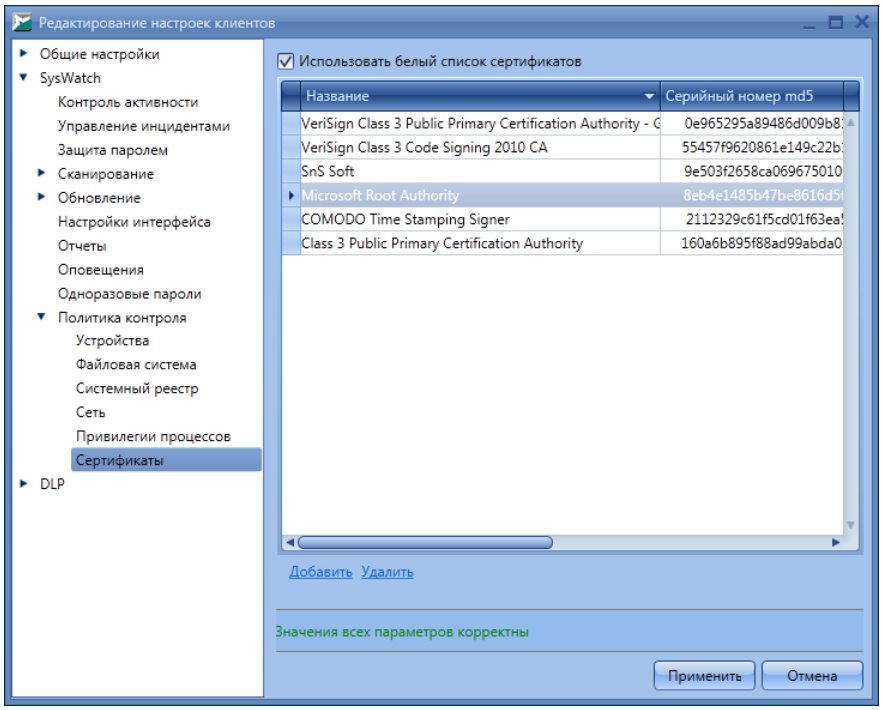


Рисунок 75. Белый список сертификатов

Изначально SoftControl SysWatch содержит базовый список сертификатов доверенных производителей. Чтобы добавить новый сертификат, нажмите на ссылку

Добавить и укажите приложение, программу установки или сценарий, подписанный ЭЦП, сертификат которого требуется включить в перечень, после чего нажмите на кнопку **Открыть**. В появившемся окне со списком сертификатов ЭЦП выбранного файла установите флажки в столбце **Добавить** для требуемых сертификатов и нажмите на кнопку **OK** (рис. Выбор сертификатов для добавления 88). Установите флажок в столбце **Доверять** для добавленных сертификатов (рис. Белый список сертификатов 87).

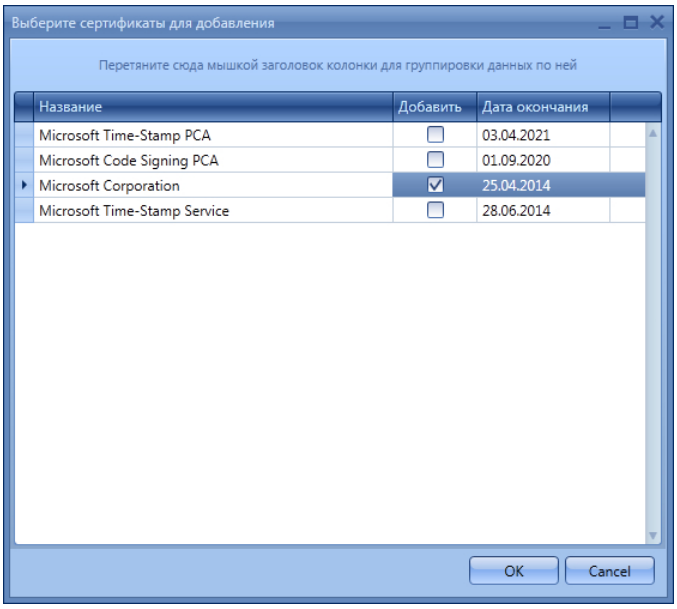


Рисунок 76. Выбор сертификатов для добавления

Если необходимо исключить сертификат из перечня доверенных без его удаления, сбросьте флажок в столбце **Доверять**. Для полного удаления сертификата из списка выберите его и нажмите на ссылку **Удалить** (рис. Белый список сертификатов 87).

4.6.3 Настройки SoftControl DLP Client

Данная категория настроек включает в себя конфигурацию клиентского компонента SoftControl DLP Client.

Сбор данных

В разделе **Сбор данных** категории **DLP** установите флажок **Собирать данные** и отметьте необходимые области собираемой информации (рис. Настройки сбора данных 89):

- ❑ **Время работы с приложением**;
- ❑ **Использование USB устройств**;
- ❑ **Печать документов**;
- ❑ **Пересылка документов по почте**;
- ❑ **Ввод текста с клавиатуры**.

Наблюдение за файловой системой [90], системным реестром [92] и сетевым трафиком [94] активно при выставленной опции **Собирать данные** и заданном правиле (правилах) в соответствующих пунктах раздела **Наблюдение**.

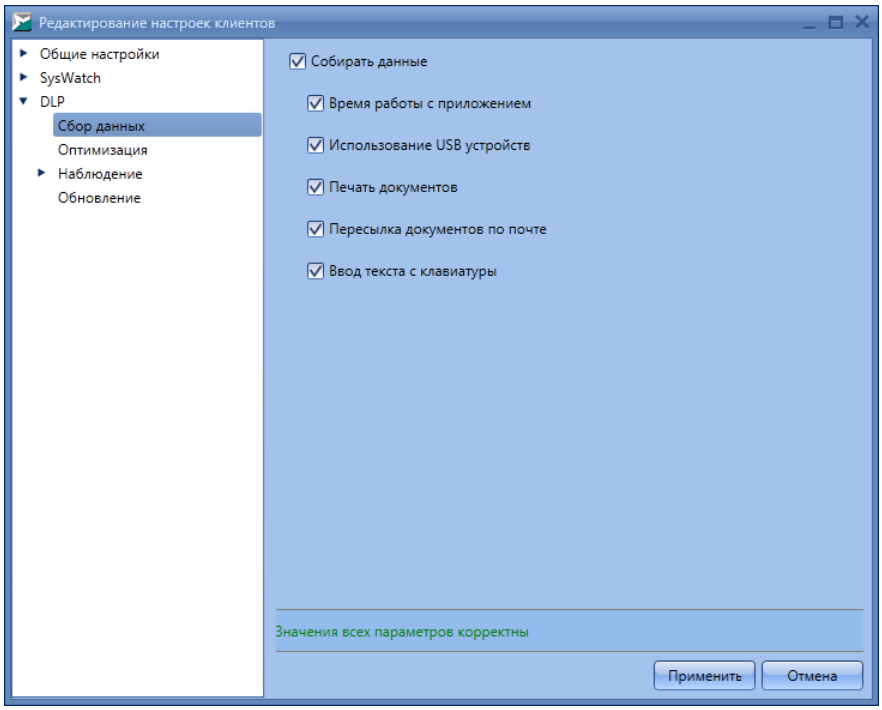


Рисунок 77. Настройки сбора данных

Оптимизация

В разделе **Оптимизация** категории **DLP** задаются временные параметры регистрации событий (рис. Настройки оптимизации [89]).

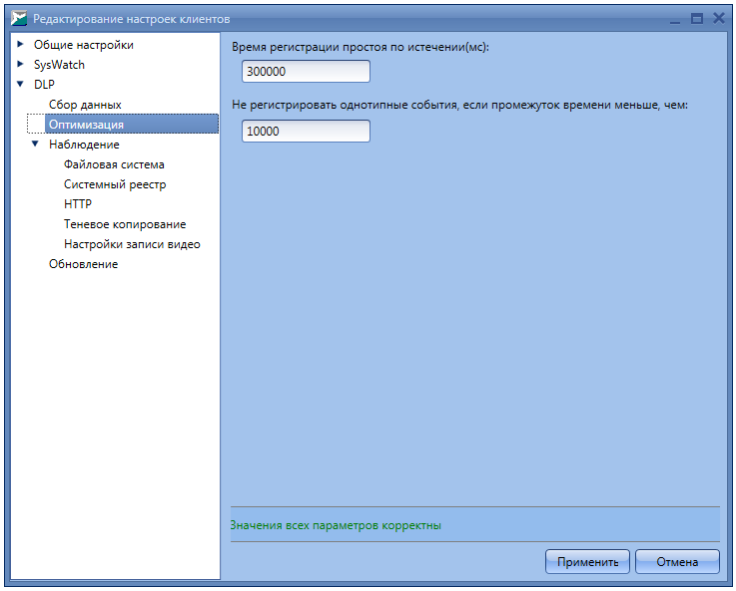


Рисунок 78. Настройки оптимизации

В соответствующих полях задайте временные интервалы **Время регистрации простоя по истечении (мс)** и **Не регистрировать однотипные события, если промежуток времени меньше, чем** в миллисекундах.

Примечание: опция **Не регистрировать однотипные события, если промежуток времени (мс) меньше чем** применяется только при наблюдении за ресурсами файловой системы. Опция **Время регистрации простоя по истечении (мс)** работает при включённой опции **Время работы с приложением** (см. рис. Настройки сбора данных[89]) и учитывает время простоя активного приложения, когда пользователь не нажимает на кнопки и не двигает мышью в течение указанного времени.

Наблюдение: Файловая система

В разделе **Наблюдение** → **Файловая система** категории **DLP** осуществляется выбор объектов файловой системы для наблюдения (рис. Настройки наблюдения за файловой системой[91]).

Чтобы добавить объект для наблюдения, нажмите на кнопку ✚ (**Добавить**) и введите полный путь до него в появившемся окне (рис. Объект наблюдения[92]). Вы можете указывать как папки на локальном жёстком диске, так и сетевые папки.

Вы можете использовать маски – инструмент задания правил для группы объектов файловой системы. Например, с помощью масок можно создать правило для каталога и всех объектов внутри него или правило для определённых типов

(расширений) файлов. Ниже приведён синтаксис масок:

- **#*#** – заменяет любое количество символов, кроме символа '\' (в случае размещения в конце строки распространяется только на файлы корневой директории);
- **#**#** – заменяет любое количество символов (в случае размещения в конце строки распространяется на файлы корневой директории, поддиректории и файлы поддиректорий);
- **#?#** – заменяет ровно 1 любой символ.

Например, чтобы установить наблюдение за каталогом и всеми вложенными объектами, добавьте символы #**# в конец строки. Нажмите на кнопку **OK** для добавления указанного объекта в список.

Чтобы изменить путь к объекту, выберите его в списке и нажмите на кнопку (**Изменить**). Для удаления объекта из под наблюдения выберите его и нажмите на кнопку (**Удалить**).

Для каждого объекта возможен выбор следующих операций, которые должны быть зарегистрированы в отчётах:

- ❑ **Чтение**;
- ❑ **Создание**;
- ❑ **Удаление**;
- ❑ **Переименование**;
- ❑ **Изменение**.

В случае переименования объекта на клиентском хосте дальнейшее наблюдение за ним не производится.

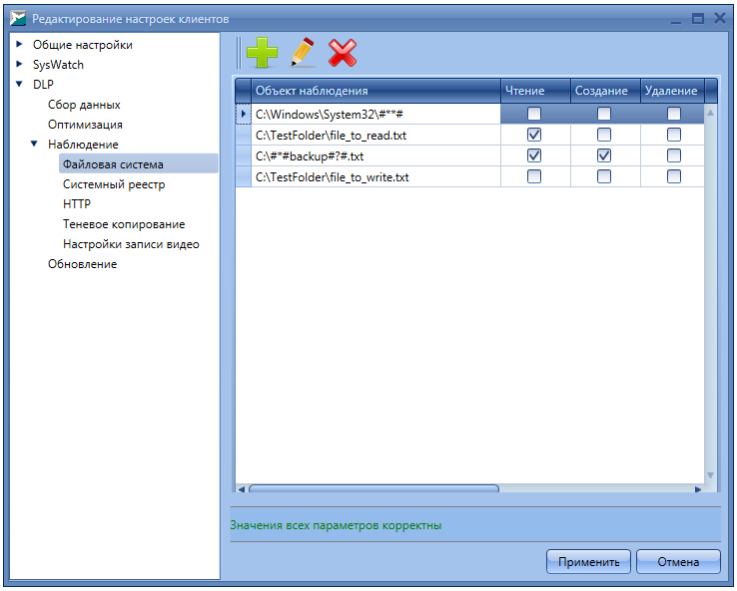


Рисунок 79. Настройки наблюдения за файловой системой

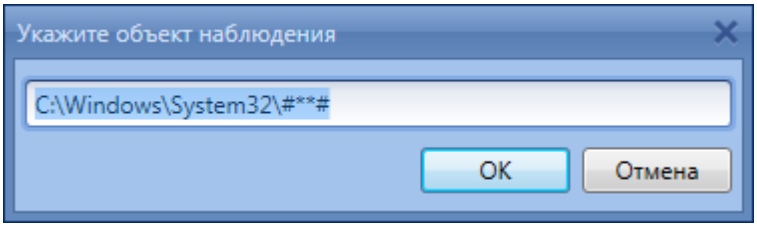


Рисунок 80. Объект наблюдения

При установке опции **Теневая копия** будет осуществляться сохранение резервной копии наблюдаемого объекта перед его модификацией, в случае включенной глобальной опции теневого копирования[95] и выставленной галочке в полях **Удаление** или **Изменение**. При установке опции **Запись видео** будет производиться сохранение снимков экрана клиентского хоста с заданными параметрами[96] в момент возникновения наблюдаемого события.

Наблюдение: Системный реестр

В разделе **Наблюдение** → **Системный реестр** категории **DLP** осуществляется выбор объектов системного реестра для наблюдения (рис. Настройки наблюдения за системным реестром[92]).

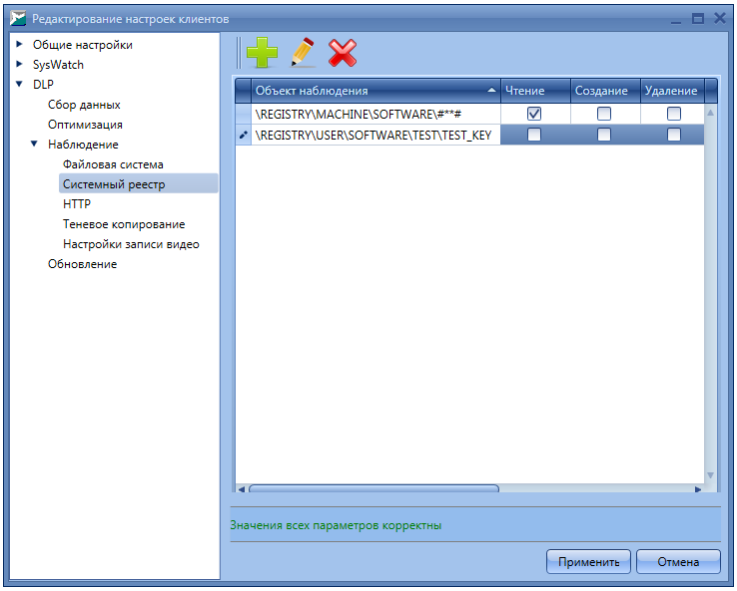


Рисунок 81. Настройки наблюдения за системным реестром

Чтобы добавить объект для наблюдения, нажмите на кнопку ✚ (**Добавить**) и введите полный путь до него в появившемся окне (рис. Объект наблюдения 94), при этом корневые разделы реестра в задаваемом пути должны быть указаны следующим образом:

- *\REGISTRY\MACHINE\SOFTWARE\CLASSES* – раздел HKEY_CLASSES_ROOT;
- *\REGISTRY\MACHINE* – раздел HKEY_LOCAL_MACHINE;
- *\REGISTRY\USER\<SID>* – раздел HKEY_CURRENT_USER для пользователя с указанным идентификатором безопасности (<SID>);
- *\REGISTRY\USER* – раздел HKEY_USERS.

Вы можете использовать маски – инструмент задания правил для группы объектов системного реестра. Например, с помощью масок можно создать правило для раздела реестра и всех объектов внутри него. Ниже приведён синтаксис масок:

- **#*#** – заменяет любое количество символов, кроме символа '\' (в случае размещения в конце строки распространяется только на параметры раздела);
- **#**#** – заменяет любое количество символов (в случае размещения в конце строки распространяется на параметры раздела, подразделы и параметры подразделов);
- **#?#** – заменяет ровно 1 любой символ.

Например, чтобы установить наблюдение за ключом реестра и всеми вложенными

объектами, добавьте символы #**# в конец строки. Нажмите на кнопку **OK** для добавления указанного объекта в список.

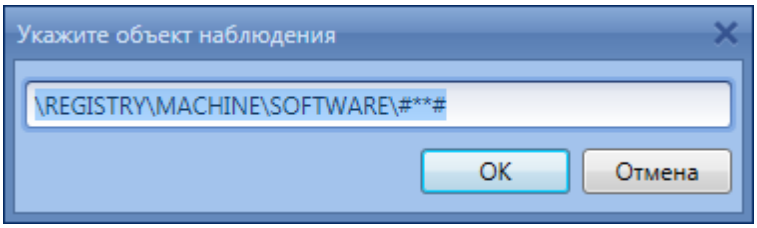


Рисунок 82. Объект наблюдения

Чтобы изменить путь к объекту, выберите его в списке и нажмите на кнопку (**Изменить**). Для удаления объекта из под наблюдения выберите его и нажмите на кнопку (**Удалить**).

Для каждого объекта возможен выбор следующих операций, которые должны быть зарегистрированы в отчётах:

- **Чтение**;
- **Создание**;
- **Удаление**;
- **Переименование**;
- **Изменение**.

В случае переименования объекта на клиентском хосте дальнейшее наблюдение за ним не производится.

При установке опции **Теневая копия** будет осуществляться сохранение резервной копии наблюдаемого объекта перед его модификацией, в случае включенной глобальной опции теневого копирования 95 и выставленной галочке в полях **Удаление** или **Изменение**. При установке опции **Запись видео** будет производиться сохранение снимков экрана клиентского хоста с заданными параметрами 96 в момент возникновения наблюдаемого события.

Наблюдение: HTTP-трафик

В разделе **Наблюдение** → **HTTP** категории **DLP** осуществляется задание наблюдаемых данных в сетевом трафике (рис. Настройки наблюдения за сетевым траффиком 94).

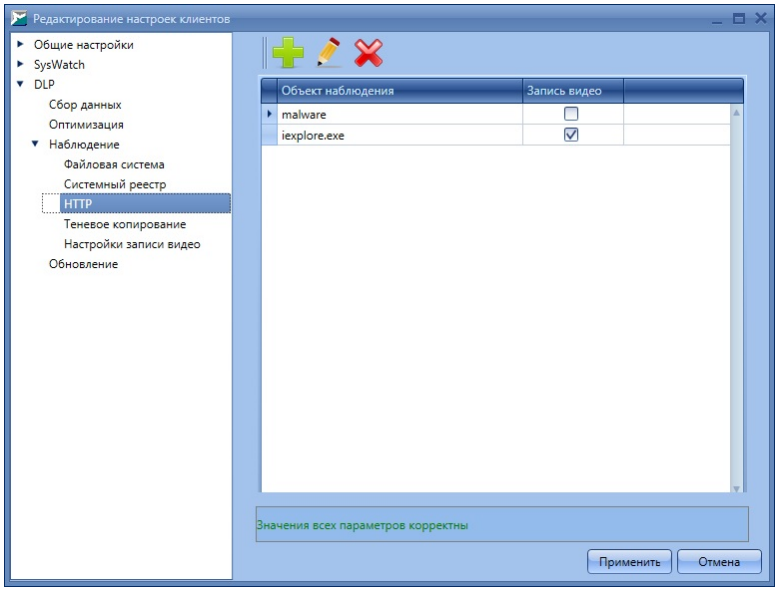


Рисунок 83. Настройки наблюдения за сетевым траффиком

Чтобы добавить данные для наблюдения, нажмите на кнопку ✚ (**Добавить**) и введите строку в появившемся окне (рис. Объект наблюдения 95). Наличие указанного текста будет отслеживаться при передаче данных по протоколу HTTP. В том числе это могут быть запросы пользователя в поисковых системах через интернет-браузер или имя файла, передаваемого по сети. Нажмите на кнопку **OK** для добавления строки в список.

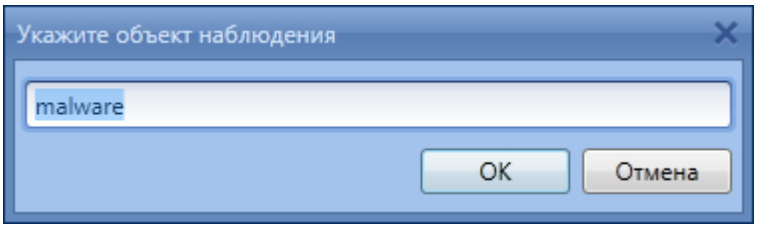


Рисунок 84. Объект наблюдения

Чтобы изменить отслеживаемый текст, выберите строку в списке и нажмите на кнопку (**Изменить**). Для удаления текста из под наблюдения выберите строку в списке и нажмите на кнопку ✖ (**Удалить**).

При установке опции **Запись видео** будет производиться сохранение снимков экрана клиентского хоста с заданными параметрами 96 в момент возникновения наблюдаемого события.

Наблюдение: Теневое копирование

В разделе **Наблюдение** → **Теневое копирование** категории **DLP** осуществляется настройка сохранения теневых копий наблюдаемых объектов (рис. Настройки

теневого копирования[96]).

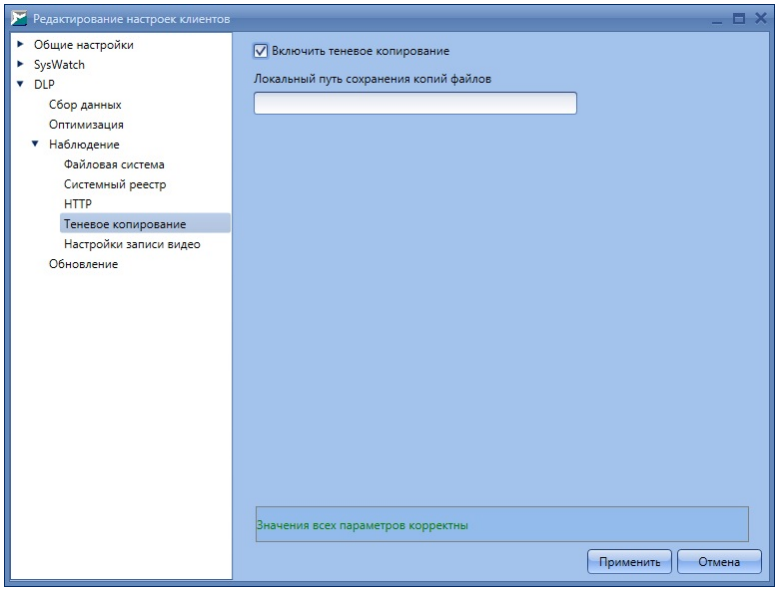


Рисунок 85. Настройки теневого копирования

Установите флажок **Включить теневое копирование** для включения функции сохранения резервных копий наблюдаемых объектов файловой системы[90] и системного реестра[92] в случае их изменения. Индивидуальная настройка по включению данной опции для отдельных объектов задаётся в свойствах наблюдения. Теневые копии объектов передаются на сервер и доступны через консоль управления. Они также сохраняются локально на клиентских хостах с установленным SoftControl DLP Client по пути, указанному в поле **Локальный путь сохранения копий файлов** или в следующий каталог по умолчанию, если путь не указан:

```
<каталог установки SoftControl DLP Client>\Backups
```

Наблюдение: Настройки записи видео

В разделе **Наблюдение** → **Настройки записи видео** категории **DLP** осуществляется настройка сохранения снимков экрана при возникновении наблюдаемых событий (рис. Настройки записи видео[96]).

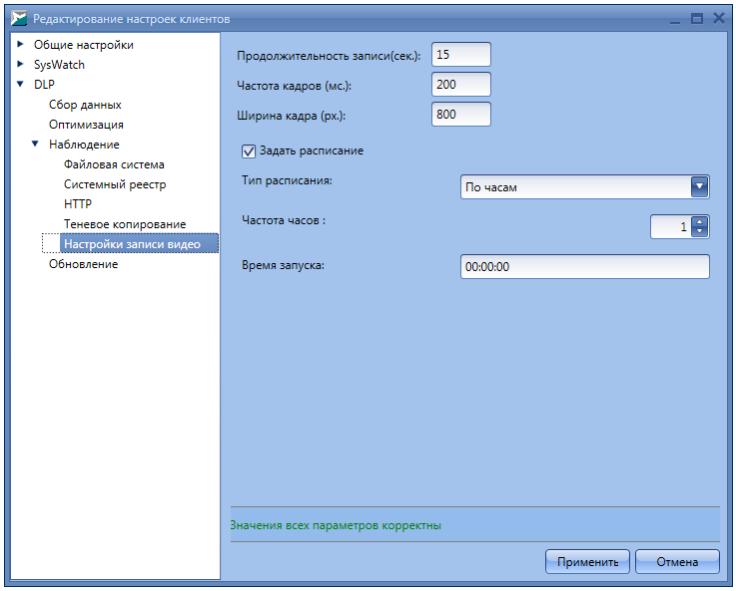


Рисунок 86. Настройки записи видео

Задайте следующие параметры записи:

- **Продолжительность записи** – длительность сохранения снимков экрана, начиная с момента возникновения события (диапазон значений: 5-60 с);
- **Частота кадров** – временной интервал между сохранением снимков экрана (диапазон значений: 50-500 мс);
- **Ширина кадра** – ширина снимка экрана в пикселах (диапазон значений: 0-1920).

Чтобы начать запись видео в режиме реального времени, щёлкните правой кнопкой мыши по требуемому клиентскому приложению SoftControl DLP Client на вкладке Устройства и статусы 39 и в контекстном меню выберите команду **Начать запись видео**.

Вы можете включить запись видео по расписанию, выставив галочку **Задать расписание**. В этом случае задайте следующие параметры записи:

- **Тип расписания** – по дням или по часам;
- **Частота дней/Частота часов** – периодичность, с которой будет выполняться задача;
- **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс*.

Настройки обновления

В разделе **Обновление** категории **DLP** возможно установить расписание обновления, для этого установите флажок **Задать расписание** и настройте параметры (рис. Настройки расписания обновления 98).

Выберите тип расписания – **По дням** или **По часам**, в счётчике **Частота дней/ Частота часов** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс*.

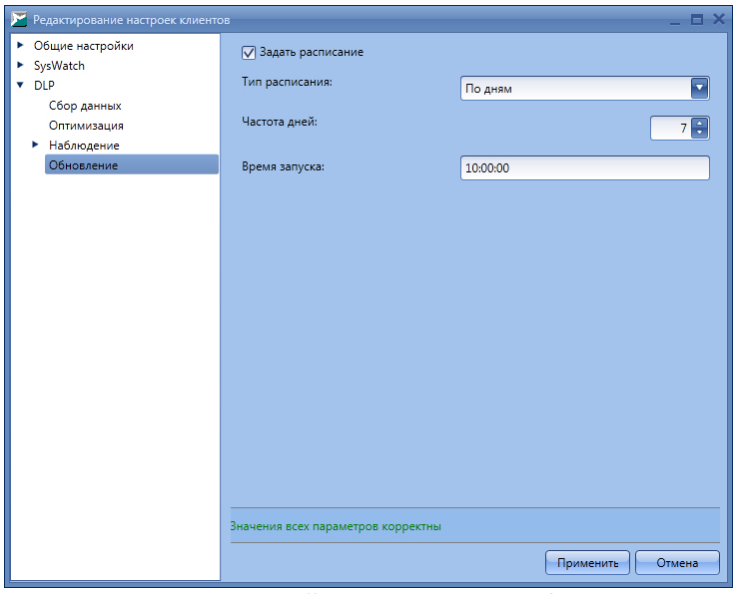


Рисунок 87. Настройки расписания обновления

4.7 Задачи

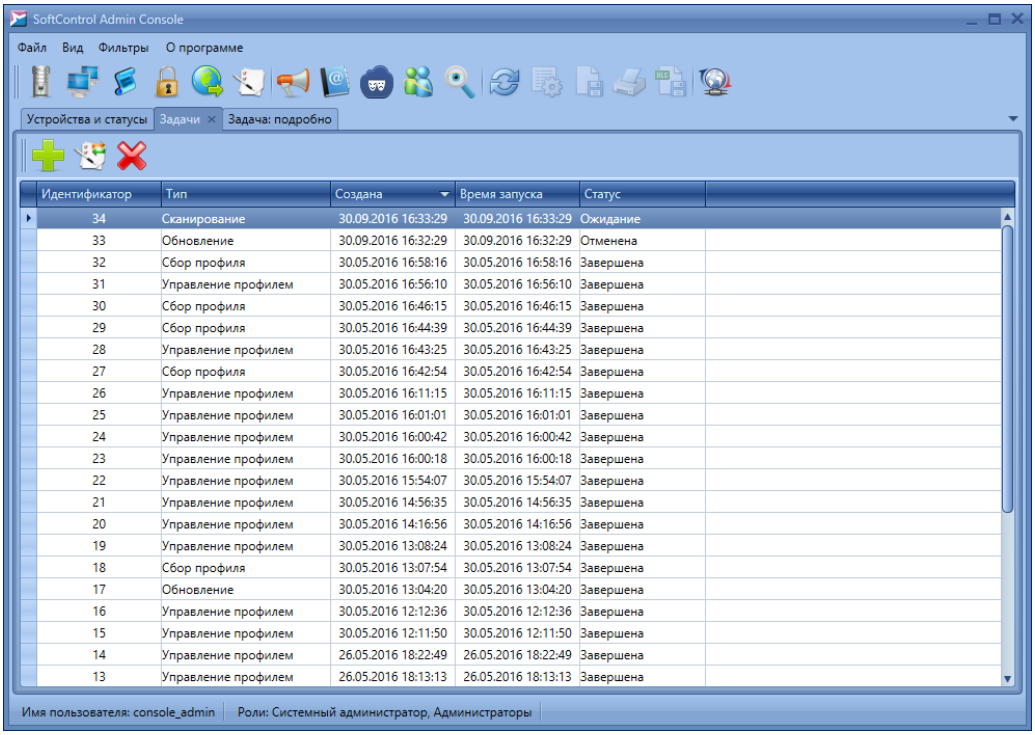
Вкладка **Задачи** позволяет создавать задачи для клиентских приложений и отслеживать детали их выполнения (рис. Вкладка "Задачи" 98).

На вкладке представлен список всех задач и их параметры.

Основные операции с задачами осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 16.

Таблица 16. Элементы управления вкладки "Задачи"

Кнопка	Название	Описание
	Создать	Создание задачи для клиентских компонентов.
	Подробная информация	Просмотр отчёта о выполнении выбранной задачи.
	Отменить	Отмена задачи, находящейся в статусе **ожидание**.



Идентификатор	Тип	Создана	Время запуска	Статус
34	Сканирование	30.09.2016 16:33:29	30.09.2016 16:33:29	Ожидание
33	Обновление	30.09.2016 16:32:29	30.09.2016 16:32:29	Отменена
32	Сбор профиля	30.05.2016 16:58:16	30.05.2016 16:58:16	Завершена
31	Управление профилем	30.05.2016 16:56:10	30.05.2016 16:56:10	Завершена
30	Сбор профиля	30.05.2016 16:46:15	30.05.2016 16:46:15	Завершена
29	Сбор профиля	30.05.2016 16:44:39	30.05.2016 16:44:39	Завершена
28	Управление профилем	30.05.2016 16:43:25	30.05.2016 16:43:25	Завершена
27	Сбор профиля	30.05.2016 16:42:54	30.05.2016 16:42:54	Завершена
26	Управление профилем	30.05.2016 16:11:15	30.05.2016 16:11:15	Завершена
25	Управление профилем	30.05.2016 16:01:01	30.05.2016 16:01:01	Завершена
24	Управление профилем	30.05.2016 16:00:42	30.05.2016 16:00:42	Завершена
23	Управление профилем	30.05.2016 16:00:18	30.05.2016 16:00:18	Завершена
22	Управление профилем	30.05.2016 15:54:07	30.05.2016 15:54:07	Завершена
21	Управление профилем	30.05.2016 14:56:35	30.05.2016 14:56:35	Завершена
20	Управление профилем	30.05.2016 14:16:56	30.05.2016 14:16:56	Завершена
19	Управление профилем	30.05.2016 13:08:24	30.05.2016 13:08:24	Завершена
18	Сбор профиля	30.05.2016 13:07:54	30.05.2016 13:07:54	Завершена
17	Обновление	30.05.2016 13:04:20	30.05.2016 13:04:20	Завершена
16	Управление профилем	30.05.2016 12:12:36	30.05.2016 12:12:36	Завершена
15	Управление профилем	30.05.2016 12:11:50	30.05.2016 12:11:50	Завершена
14	Управление профилем	26.05.2016 18:22:49	26.05.2016 18:22:49	Завершена
13	Управление профилем	26.05.2016 18:13:13	26.05.2016 18:13:13	Завершена

Рисунок 88. Вкладка "Задачи"

Перечень полей вкладки приведён в табл. 17.

Таблица 17. Поля вкладки "Задачи"

Поле	Описание
Идентификатор	Порядковый номер задачи.
Тип задачи	Тип задачи: • **сбор профиля**; • **сканирование**; • **обновление**.
Создана	Дата и время создания задачи.
Время запуска	Дата и время запуска задачи.
Статус	Статус завершения задачи: • **ожидание** – выполнение задачи не начал ни один клиентский компонент; • **отменена** – задача была отменена до начала выполнения; • **выполняется** – выполнение задачи начато как минимум одним из клиентских компонентов; • **завершена** – задача выполнена всеми клиентскими компонентами.

Основные действия, выполняемые на данной вкладке:

Создание задачи

Чтобы добавить новую задачу, нажмите на кнопку **Создать** (рис. Вкладка "Задачи" 98).

В окне **Новая задача** задайте параметры задачи в зависимости от её типа (см. рисунки, начиная с Шаг "Тип задачи" 101 и до Шаг "Клиенты" 105 в разделе Обновление 104):

- сбор профиля[101];
- антивирусное сканирование[102];
- обновление[104].

Просмотр подробностей выполнения задачи

Чтобы просмотреть подробности выполнения задачи, выберите её и выполните одно из следующих действий:

- нажмите на кнопку **Подробная информация** в группе кнопок вкладки (рис. Вкладка "Задачи"[98]);
- дважды нажмите левой кнопки мыши на задаче.

В появившейся дополнительной вкладке **Задача: подробно** приведена детальная информация по задаче и ход выполнения для каждого клиентского компонента в отдельности (рис. Подробности выполнения задачи[100]).

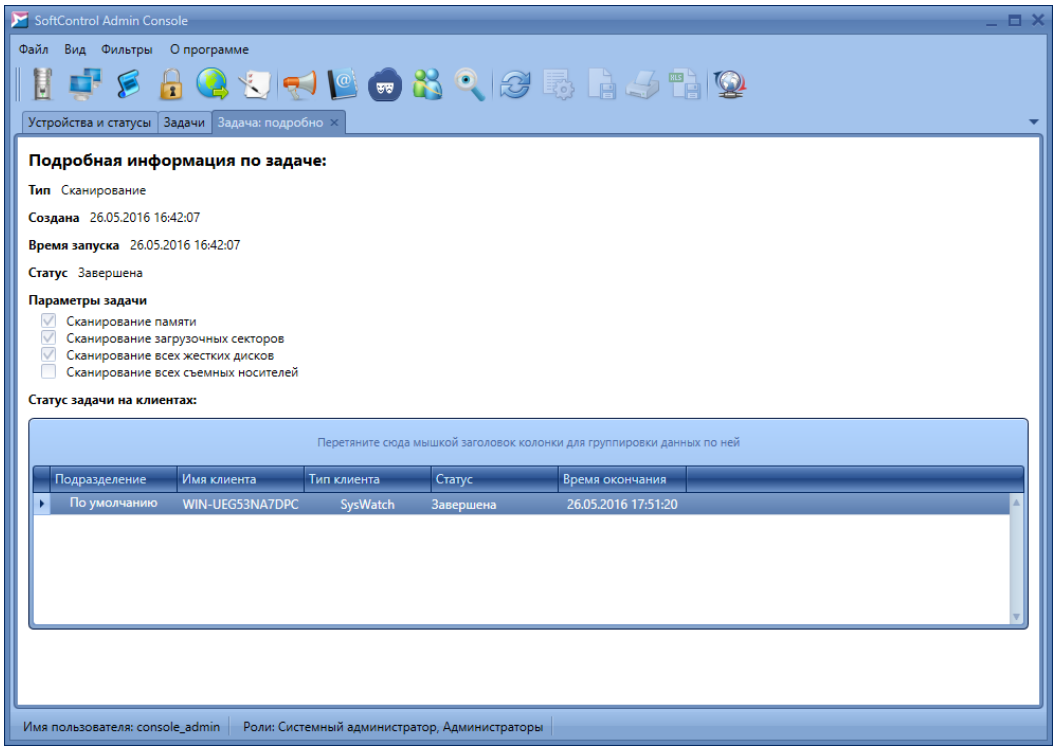


Рисунок 89. Подробности выполнения задачи

Помимо основной информации (табл. 17) и параметров задачи, на вкладке отображается дополнительная таблица **Статус задачи на клиентах**, описание полей которой дано в табл. 18.

Таблица 18. Поля таблицы "Статус задачи на клиентах"

Поле	Описание
Подразделение	Подразделение, к которому относится клиентский компонент.
Имя клиента	NetBIOS-имя клиентского хоста.
Статус	Статус завершения задачи для данного клиентского компонента: • **ожидание** – выполнение задачи не начато; • **запуск** – клиентскому компоненту успешно отправлена команда на запуск задачи; • **ошибка запуска** – клиентский компонент не смог произвести запуск задачи; • **выполняется** – задача находится в процессе выполнения клиентским компонентом; • **ошибка выполнения** – в процессе выполнения задачи возникла ошибка; • **отменена** – задача была отменена; • **завершена** – выполнение задачи завершено; • **ошибка завершения** – при завершении задачи возникла ошибка.
Время окончания	Время завершения задачи на данном клиентском хосте.

Чтобы просмотреть отчёты непосредственно по выполненным операциям, перейдите на вкладку **Лог** и примените фильтры 119 для соответствующих типов операций.

4.7.1 Сбор профиля

1) На шаге **Тип задачи** выберите **Сбор профиля** в выпадающем списке и нажмите на кнопку **Вперед** (рис. Шаг "Тип задачи" 101).

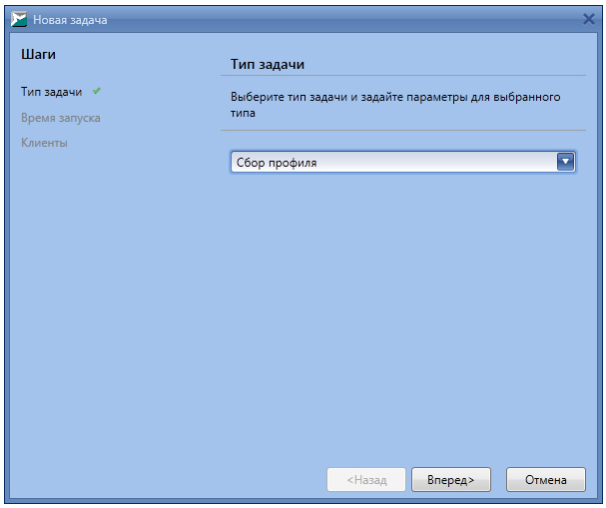


Рисунок 90. Шаг "Тип задачи"

2) На шаге **Время запуска** выберите опцию **Сейчас** для немедленного запуска задачи после её добавления, либо выберите опцию **Указать время** и определите дату и время

запуска (рис. Шаг "Время запуска" 102). Нажмите на кнопку **Вперед** для продолжения.

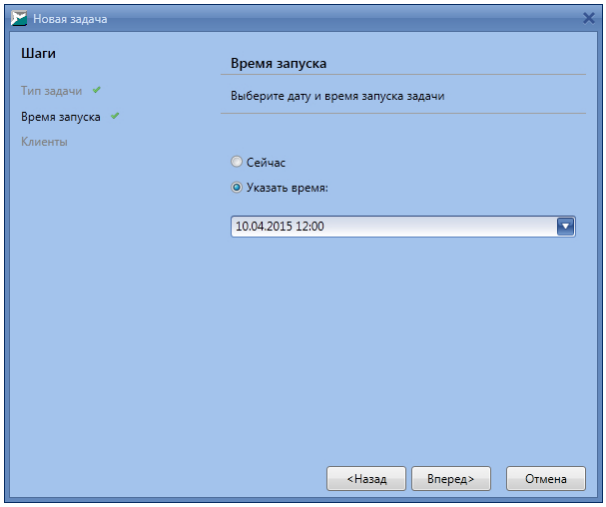


Рисунок 91. Шаг "Время запуска"

3) На шаге **Клиенты** отметьте клиентские компоненты, для которых необходимо создать задачу (рис. Шаг "Клиенты" 102). При выборе типа клиента **SysWatch** задача будет назначена всем клиентским компонентам, при выборе подразделения – всем клиентским компонентам подразделения. Нажмите на кнопку **Готово**, чтобы создать задачу, или на кнопку **Назад**, если требуется изменить параметры задачи.

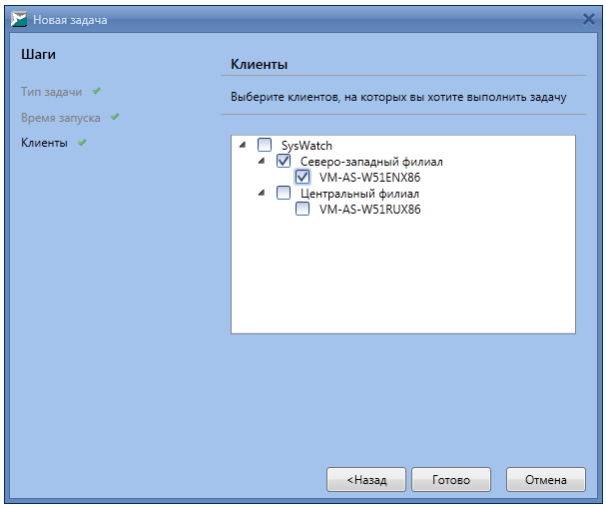


Рисунок 92. Шаг "Клиенты"

4.7.2 Антивирусное сканирование

1) На шаге **Тип задачи** выберите **Сканирование** в выпадающем списке и отметьте области клиентского хоста для антивирусной проверки (рис. Шаг "Тип задачи" 103):

- ❑ **Сканирование памяти**;

- ❑ **Сканирование загрузочных секторов**;
- ❑ **Сканирование всех жестких дисков**;
- ❑ **Сканирование всех съемных носителей**.

Нажмите на кнопку **Вперед** для продолжения.

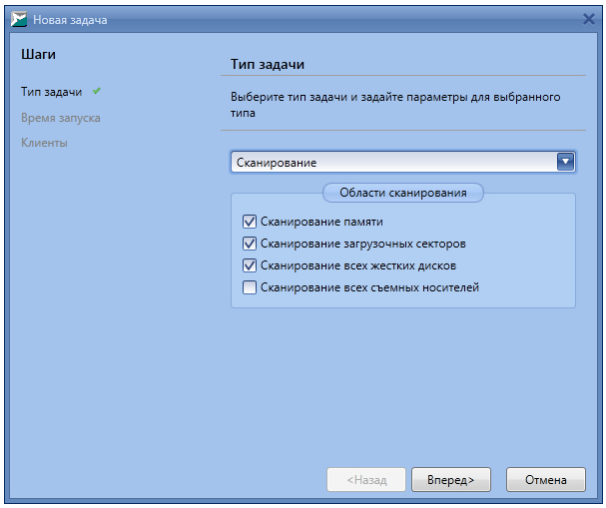


Рисунок 93. Шаг "Тип задачи"

2) На шаге **Время запуска** выберите опцию **Сейчас** для немедленного запуска задачи после её добавления, либо выберите опцию **Указать время** и определите дату и время запуска (рис. Шаг "Время запуска" 103). Нажмите на кнопку **Вперед** для продолжения.

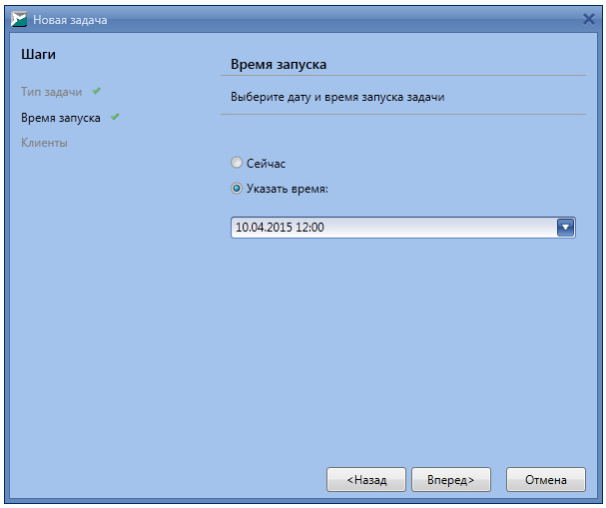


Рисунок 94. Шаг "Время запуска"

3) На шаге **Клиенты** отметьте клиентские компоненты, для которых необходимо создать задачу (рис. Шаг "Клиенты" 103).

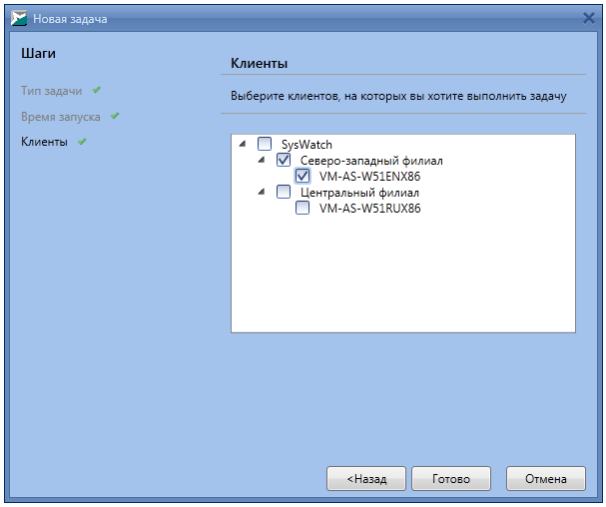


Рисунок 95. Шаг "Клиенты"

При выборе типа клиента **SysWatch** задача будет назначена всем клиентским компонентам, при выборе подразделения – всем клиентским компонентам подразделения. Нажмите на кнопку **Готово**, чтобы создать задачу, или на кнопку **Назад**, если требуется изменить параметры задачи.

4.7.3 Обновление

1) На шаге **Тип задачи** выберите **Обновление** в выпадающем списке и отметьте необходимые компоненты для обновления и параметры задачи (рис. Шаг "Тип задачи" 104):
   - ❑ **Программные модули** – обновление программных модулей компонентов типа SysWatch и DLP.
   - ❑ **Антивирусные базы** – обновление антивирусных баз компонентов типа SysWatch.
   - ❑ **Выполнить перезагрузку клиентов** – перезагрузка клиентских хостов по окончании обновления. Если данная опция не выбрана, то для завершения обновления программных модулей перезагрузку необходимо выполнить локально вручную на клиентском хосте, что отображается в статусе компонента на вкладке Устройства и статусы 39 и событиях обновления в отчётах 106.

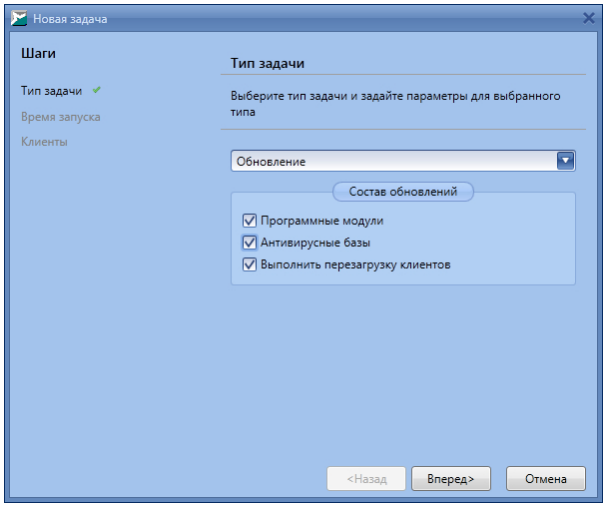


Рисунок 96. Шаг "Тип задачи"

Нажмите на кнопку **Вперед** для продолжения.

2) На шаге **Время запуска** выберите опцию **Сейчас** для немедленного запуска задачи после её добавления, либо выберите опцию **Указать время** и определите дату и время запуска (рис. Шаг "Время запуска" 105). Нажмите на кнопку **Вперед** для продолжения.

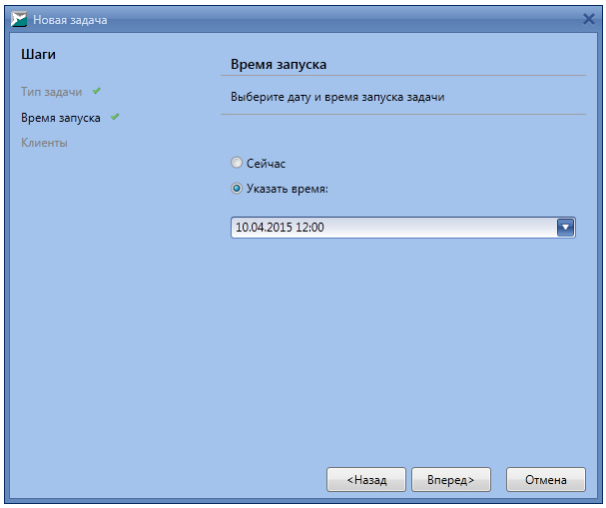


Рисунок 97. Шаг "Время запуска"

3) На шаге **Клиенты** отметьте клиентские компоненты, для которых необходимо создать задачу (рис. Шаг "Клиенты" 105). При выборе типа клиента задача будет назначена всем клиентским компонентам данного типа, при выборе подразделения – всем клиентским компонентам подразделения. Нажмите на кнопку **Готово**, чтобы создать задачу, или на кнопку **Назад**, если требуется изменить параметры задачи.

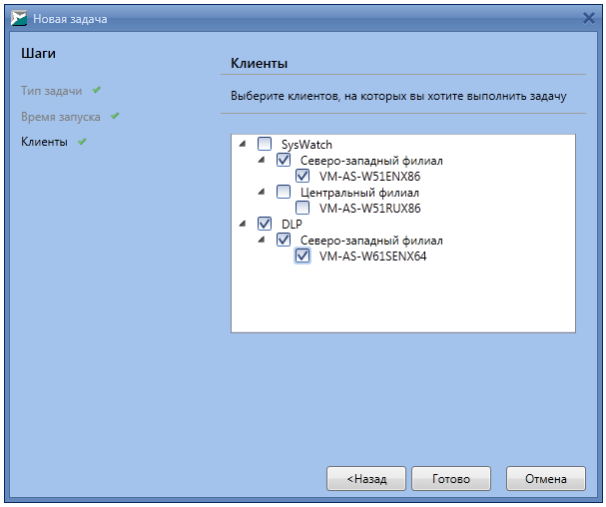


Рисунок 98. Шаг "Клиенты"

4.8 Просмотр отчётов

Для просмотра отчётов клиентских приложений в агрегированном виде через консоль управления SoftControl Admin Console предназначена вкладка **Лог**. Она позволяет в реальном времени отслеживать события на нескольких клиентских хостах одновременно и производить выборку необходимых данных с помощью гибкого механизма фильтрации[118]. На вкладке администратор получает доступ к следующим данным в удобной форме:

- Отчёты SoftControl SysWatch[106];
- Отчёты SoftControl DLP Client[113].

Полученные отчёты могут быть выведены на печать или экспортированы в электронный формат[123].

4.8.1 Отчёты SoftControl SysWatch

Вкладка **Лог** предоставляет возможности по детальному мониторингу событий безопасности, регистрируемых SoftControl SysWatch на клиентских хостах (рис. Вкладка "Лог" для компонента SoftControl SysWatch[106]).

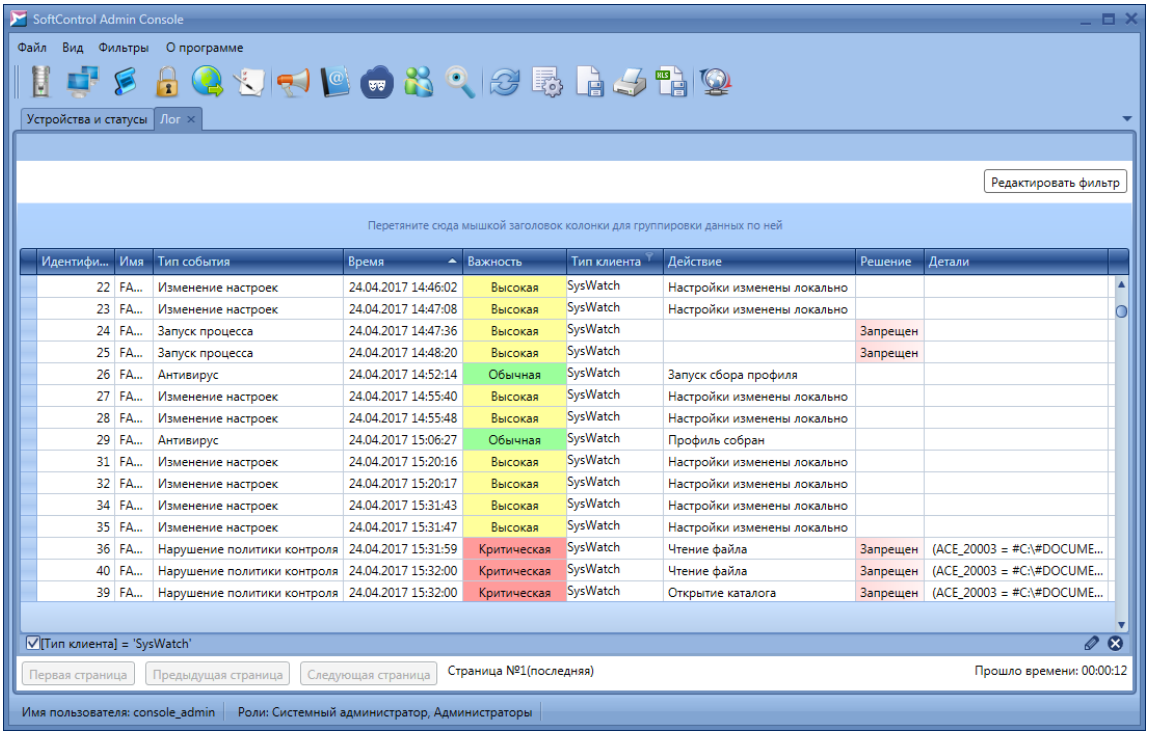


Рисунок 99. Вкладка "Лог" для компонента SoftControl SysWatch

Полный перечень полей вкладки **Лог** для компонента SoftControl SysWatch приведён в табл. 19.

Таблица 19. Поля вкладки "Лог" для SoftControl SysWatch

Поле	Описание
Имя	NetBIOS-имя клиентского хоста.
Идентификатор события	Уникальный идентификатор события. Если происходит приём события с дублированным идентификатором, дублируемая строка помечается красным цветом. В случае нарушения целостности порядка идентификаторов (разрывы в последовательности), в отчёт серверного компонента в журнале Windows 153 вносится соответствующее предупреждение. Исключением являются события типа **Статус**, для которых данный параметр принимает значения *-1* или *-2*.
Уникальный ID устройства	Уникальный идентификатор клиентского хоста, который автоматически присваивается ему при первом обращении клиентского приложения SoftControl SysWatch к серверу SoftControl Server.
Тип события	Тип события безопасности (инцидента): • **нарушение политики контроля**; • **контроль активности**; • **обновление клиента**; • **запуск процесса**; • **антивирус**; • **изменение настроек**; • **статус**; • **вход пользователя**; • **выход пользователя**.
Время	Дата и время регистрации события.

Поле	Описание
Важность	Важность (приоритет) события с точки зрения угрозы информационной безопасности клиентского хоста: • обычная; • высокая; • критическая. Каждому уровню приоритета соответствует свой цвет ячейки.
Действие	Действие в случае события типа **нарушение политики контроля**: • **чтение файла**; • **изменение файла**; • **переименование файла**; • **удаление файла**; • **открытие каталога**; • **удаление каталога**; • **открытие ключа реестра**; • **создание ключа реестра**; • **удаление ключа реестра**; • **изменение значения реестра**; • **удаление значения реестра**; • **загрузка DLL модуля**; • **введен неверный пароль**. Действие в случае события типа **запуск процесса**: • **запуск приложения**; • **запуск приложения с ЦП**; • **запуск неизвестного приложения**; • **запуск неизвестного приложения с ЦП**; • **запуск инсталлятора**; • **запуск инсталлятора с ЦП**; • **запуск инсталлятора с ЦП вне `Белого списка`**; • **запуск неизвестного инсталлятора**; • **запуск неизвестного инсталлятора с ЦП**; • **запуск неизвестного инсталлятора с ЦП вне `Белого списка`**. Действие в случае события типа **антивирус**: • **запуск сканера**; • **запуск сбора профиля**; • **завершение сканирования**; • **профиль собран**; • **сканирование объекта**. Действие в случае события типа **обновление**: • **запуск обновлений**; • **обновление завершено**. Действие в случае события типа **изменение настроек**: • **настройки изменены локально**; • **настройки изменены сервером**.
Статус действия	Статус действия в случае события типа **антивирус**: • **сканер запущен**; • **ошибка при запуске сканера**; • **сканер был остановлен**; • **успешно**;

Поле	Описание
	• **неудачно**. Статус действия в случае события типа **обновление**: • **процесс обновления запущен**; • **ошибка запуска**; • **новых обновлений не найдено**; • **обновление прервано пользователем**; • **обновления успешно установлены**; • **нужна перезагрузка системы**; • **обновление завершено с ошибками**.
Статус клиента	Статус зарегистрированного клиентского компонента: • **активен**; • **остановлен**; • **работа службы была прервана**; • **ошибка статуса. неверный статус**.
Исполняемый файл	Приложение или программа установки, вызвавшая события типов **нарушение политики контроля** или **запуск процесса**.
Командная строка процесса	– Команда, вызвавшая событие типа **запуск процесса**. – Имя объекта файловой системы/реестра, в отношении которого произошло событие типа **нарушение политики контроля**, или имя DLL-модуля, загружаемого процессом, вызвавшим событие **нарушение политики контроля**. – Неверно введённый пароль.
Пользователь	Учётная запись, под которой произошли события типов **запуск процесса** или **изменение настроек**.
Зона	Зона выполнения приложения: • **доверенные** (разрешённые); • **по умолчанию** (ограниченные); • **блокированные** (запрещенные).
Идентификатор процесса	Уникальный порядковый идентификатор процесса (PID) в ОС для события типа **запуск процесса**.
Идентификатор родительского процесса	Уникальный порядковый идентификатор родительского процесса (PPID) в ОС для события типа **запуск процесса**.
Родительский процесс	Наименование родительского процесса для события типа **запуск процесса**.
Решение	Решение по запуску приложения: • **разрешен**; • **запрещен**. Каждому решению соответствует свой цвет ячейки.
Проверено объектов	Количество объектов, проверенных в процессе антивирусного сканирования.
Угроз найдено	Количество найденных угроз в процессе антивирусного сканирования.
Угроз обезврежено	Количество обезвреженных угроз в процессе антивирусного сканирования.
Встроенные сертификаты	Количество встроенных сертификатов, обнаруженных в процессе автоматической настройки (сбора профиля).
Сертификаты каталогов	Количество сертификатов каталогов, обнаруженных в процессе автоматической настройки (сбора профиля).
Приложения	Статус контроля активности приложений: • **активно**; • **неактивно**.

Поле	Описание
Файловая система	Статус контроля файловой системы: • **активно**; • **неактивно**.
Системный реестр	Статус контроля системного реестра: • **активно**; • **неактивно**.
Сеть	Статус контроля сетевой активности: • **активно**; • **неактивно**.
Имя вошедшего пользователя	Учётная запись, под которой произошёл вход в ОС клиентского хоста.
Имя вышедшего пользователя	Учётная запись, под которой произошёл выход из ОС клиентского хоста.
Ошибка	Код ошибки в базе данных на сервере.
Тип клиента	Тип клиента, для которого отображается отчёт. Для общих событий (SysWatch и DLP) поле имеет пустое значение.
Детали	Идентификатор (UID) правила, в отношении которого произошло нарушение политики контроля.
Имя службы	Системное имя службы, которая была запущена/остановлена.
Отображаемое имя	Название службы в оснастке **Службы** ОС Windows.
Событие службы	Статус службы: • **ServiceStarted**; • **ServiceFoundRunning**; • **ServiceStopped**.

Следующие события содержат в себе расширенную информацию об инциденте:

Событие антивирусного сканера

Событие антивирусного сканера позволяет просматривать подробный отчёт о результатах проведения антивирусного сканирования [102] клиентских хостов.

Откройте список событий на вкладке **Лог** для компонента SoftControl SysWatch и выберите событие типа **Антивирус** с действием **Завершение сканирования**. Чтобы вызвать отчёт с дополнительной информацией, выполните одно из следующих действий для выбранного события:

- дважды нажмите левой кнопки мыши на событии;
- вызовите контекстное меню нажатием правой кнопки мыши на событии и выберите команду **Показать дополнительную информацию события антивируса**.

Отчёт с дополнительной информацией будет открыт только в том случае, если в результате антивирусного сканирования найдены угрозы (ненулевой счетчик в поле **Угроз найдено**) или в случае наличия необезвреженных угроз при предыдущей проверке.

В появившейся дополнительной вкладке **Сканнер** представлены все объекты, содержащие обнаруженные угрозы по результатам проверки (рис. Вкладка "Сканнер" 111).

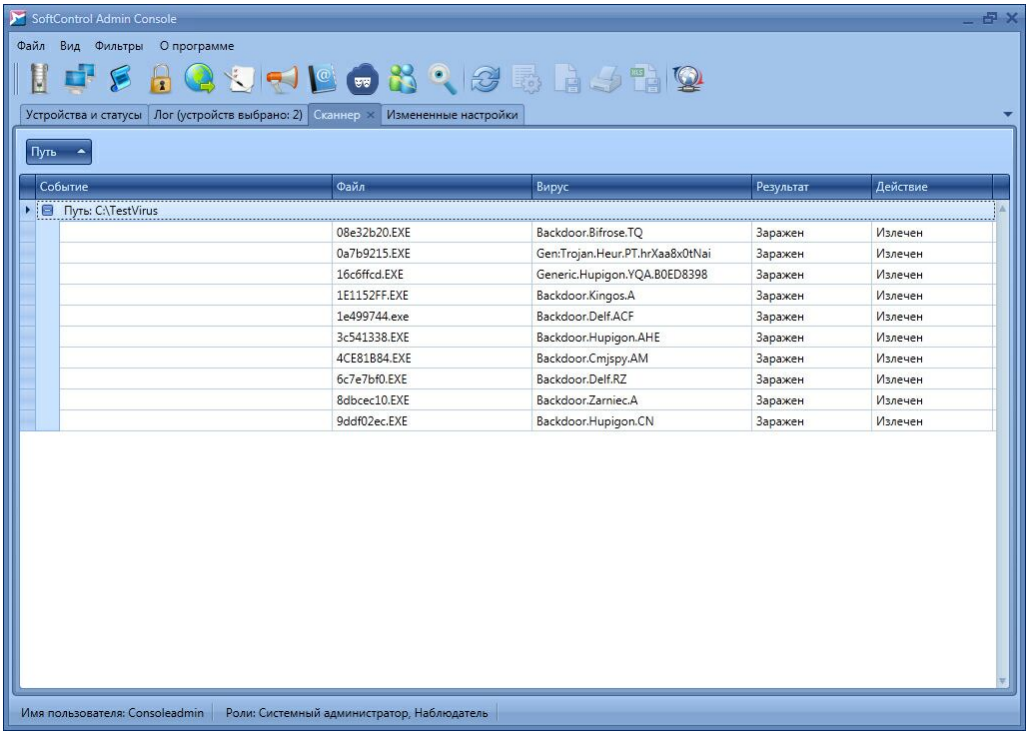


Рисунок 100. Вкладка "Сканнер"

Полный перечень полей вкладки приведён в табл. 20.

Таблица 20. Поля вкладки "Сканнер"

Поле	Описание
Событие	Дата и время окончания антивирусного сканирования.
Путь	Каталог расположения объекта в файловой системе клиентского хоста.
Файл	Имя объекта.
Вирус	Наименование вредоносного кода, которым заражён объект.
Результат	Результат антивирусного сканирования: • **Чист**; • **Заражен**; • **Подозрителен**; • **Ошибка**; • **Ошибка лечения**; • **Ошибка перемещения**; • **Ошибка удаления**.
Действие	Действие, выполненное для данного объекта по результатам антивирусного

Поле	Описание
	сканирования: • **Излечен**; • **Перемещен**; • **Пропущен**; • **Удален**; • **Нет действия**.

Событие изменения настроек

Событие изменения настроек позволяет просматривать полный список изменений в конфигурации SoftControl SysWatch. Настройки SoftControl SysWatch могут быть изменены следующими способами:

- администратором через SoftControl Admin Console [59];
- локальным пользователем с помощью:
  – ГИП программы;
  – применения конфигурационного файла.

Откройте список событий на вкладке **Лог** для компонента SoftControl SysWatch и выберите событие типа **Изменение настроек**. Чтобы вызвать отчёт с дополнительной информацией, выполните одно из следующих действий для выбранного события:

- дважды нажмите левой кнопки мыши на событии;
- вызовите контекстное меню нажатием правой кнопки мыши на событии и выберите команду **Показать дополнительную информацию события изменения настроек**.

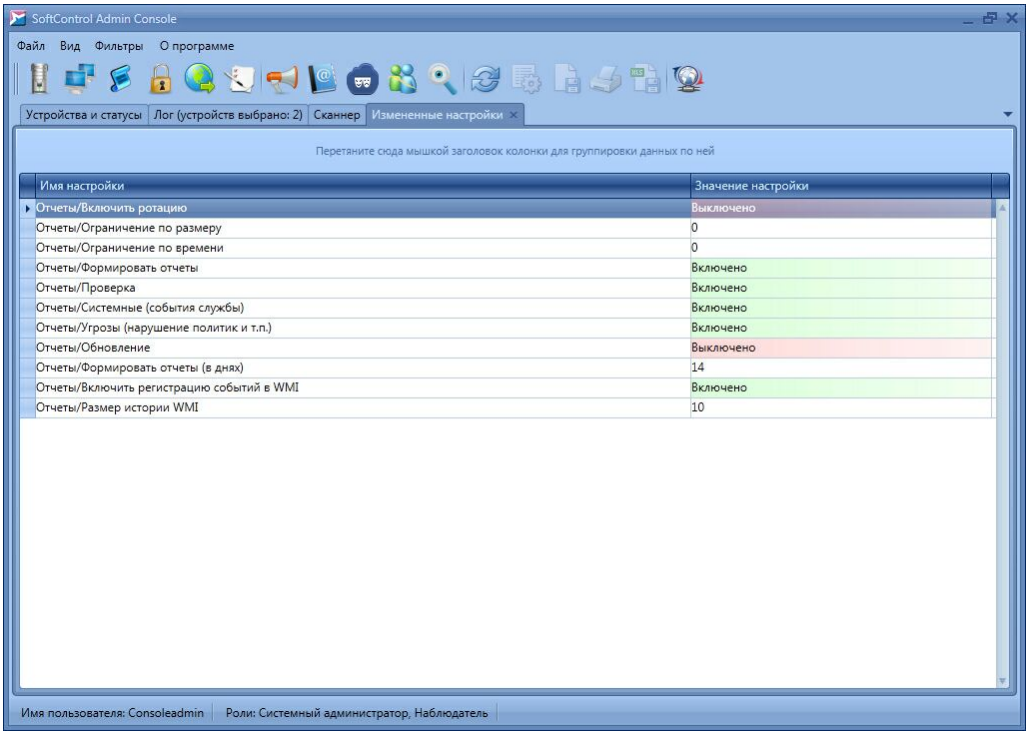


Рисунок 101. Вкладка "Измененные настройки"

В появившейся дополнительной вкладке **Измененные настройки** представлен перечень настроек SoftControl SysWatch с указанием их нового состояния (рис. Вкладка "Измененные настройки" 112).

Полный перечень полей вкладки приведён в табл. 21.

Таблица 21. Поля вкладки "Измененные настройки"

Поле	Описание
Имя настройки	Название настройки.
Значение настройки	Значение настройки, на которое оно было изменено в результате события.

4.8.2 Отчёты SoftControl DLP Client

Вкладка **Лог** предоставляет возможность просмотра отчётов по данным, собираемым SoftControl DLP Client на клиентских хостах (рис. Вкладка "Лог" для компонента SoftControl DLP Client 113).

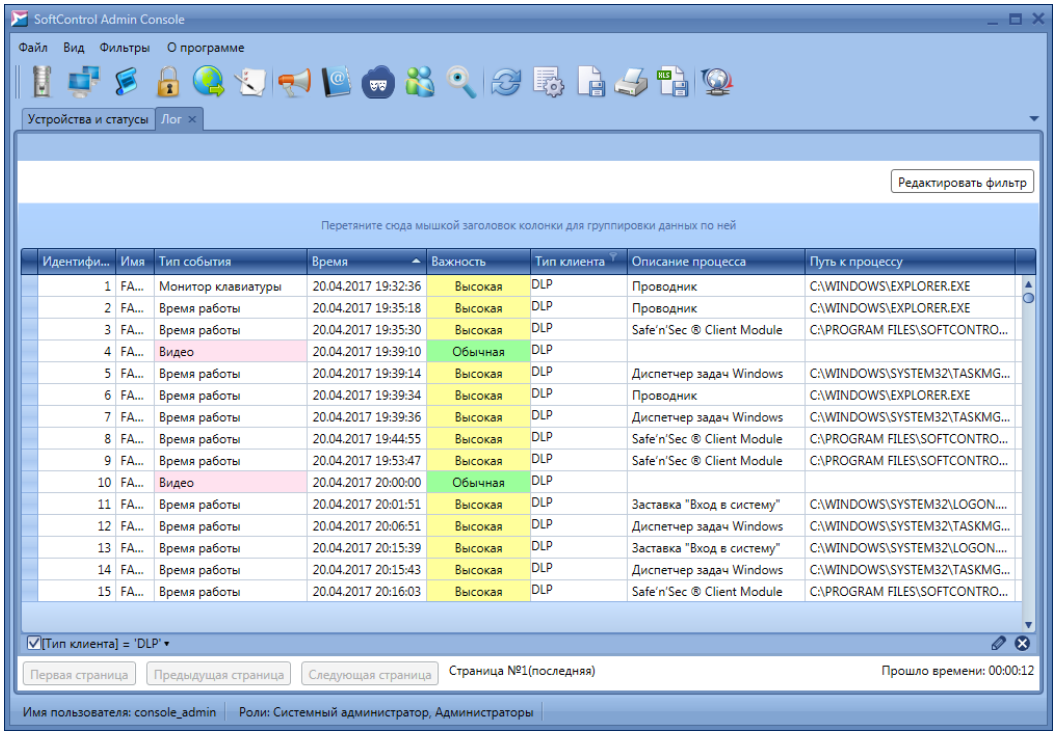


Рисунок 102. Вкладка "Лог" для компонента SoftControl DLP Client

Полный перечень полей вкладки **Лог** для компонента SoftControl DLP Client приведён в табл. 22.

Таблица 22. Поля вкладки "Лог" для SoftControl DLP Client

Поле	Описание
Имя	NetBIOS-имя клиентского хоста.
Идентификатор события	Уникальный идентификатор события. Если происходит приём события с дублированным идентификатором, дублируемая строка помечается красным цветом. В случае нарушения целостности порядка идентификаторов (разрывы в последовательности), в отчёт серверного компонента в журнале Windows 153 вносится соответствующее предупреждение. Исключением являются события типа **Статус**, для которых данный параметр принимает значения *-1* или *-2*.
Уникальный ID устройства	Уникальный идентификатор клиентского хоста, который автоматически присваивается ему при первом обращении клиентского приложения SoftControl DLP Client к серверу SoftControl Server.
Тип события	Тип события сбора данных: • **добавлено устройство**; • **вложение**; • **файл**; • **HTTP**; • **монитор клавиатуры**; • **принтер**; • **реестр**; • **устройство отсоединено**; • **время работы**.
Время	Дата и время регистрации события.

Поле	Описание
Важность	Важность (приоритет) события с точки зрения угрозы информационной безопасности клиентского хоста: • обычная; • высокая; • критическая. Каждому уровню приоритета соответствует свой цвет ячейки.
Статус клиента	Статус зарегистрированного клиентского компонента: • **активен**; • **остановлен**; • **работа службы была прервана**; • **ошибка статуса. неверный статус**.
Путь к процессу	Путь к процессу, вызвавшему событие типов **файл**, **реестр**, **HTTP**, **монитор клавиатуры**, **время работы**, **принтер**, **вложение**.
Описание процесса	Описание процесса, вызвавшего событие типов **файл**, **реестр**, **HTTP**, **монитор клавиатуры**, **время работы**, **принтер**, **вложение**.
Пользователь	Учётная запись пользователя, под которой был запущен процесс, вызвавший событие типов **файл**, **реестр**, **HTTP**, **монитор клавиатуры**, **время работы**, **принтер**, **вложение**.
IP	IP-адрес назначения HTTP-запроса для события типа **HTTP**.
Url	URL назначения HTTP-запроса для события типа **HTTP**.
Заголовок	Заголовок HTTP для события типа **HTTP**.
Маска доступа	Тип операции над наблюдаемым объектом для событий типов **файл** и **реестр**: • **чтение**; • **запись**; • **удаление**; • **переименование**; • **изменение**.
Резервная копия	Локальный путь к теневой копии наблюдаемого объекта с именем вида *<Полное имя оригинального объекта>_<N>.bkp*, где *N* – порядковый номер сохранённой копии, для событий типов **файл** и **реестр**.
Путь к файлу-вложению	Путь к файлу-вложению в почтовом клиенте Microsoft® Outlook® 2003 для события типа **вложение**.
Путь к файлу	Путь к наблюдаемому каталогу или файлу для события типа **файл**.
Тип диска	Тип носителя, на котором располагается наблюдаемый каталог или файл для события типа **файл**: • **локальный носитель**; • **съемный носитель**.
Ветка реестра	Путь к наблюдаемому разделу реестра или параметру раздела реестра для события типа **реестр**.
Время записи события	Дата записи ввода с клавиатуры для события типа **монитор клавиатуры**.
Записанные данные	Текст, введенный пользователем с клавиатуры, для события типа **монитор клавиатуры**.
Детали	Описание источника печати для события типа **принтер**.
ID устройства	ID периферийного устройства для событий типов **добавлено устройство** и **устройство отсоединено**.
Класс устройства	Класс периферийного устройства для событий типов **добавлено устройство** и **устройство отсоединено**.

Поле	Описание
Описание устройства	Описание периферийного устройства для событий типов **добавлено устройство** и **устройство отсоединено**.
Время старта	Время начала работы с приложением для события типа **время работы**.
Время окончания	Время окончания работы с приложением для события типа **время работы**.
Продолжительность	Продолжительность работы с приложением для события типа **время работы**.
Индекс файла	Индекс файла для событии типа **HTTP**.
Тип клиента	Тип клиента, для которого отображается отчёт. Для общих событий (SysWatch и DLP) поле имеет пустое значение.

События типов **файл**, **реестр** и **HTTP** выделяются в отчётах цветом, если содержат в себе дополнительные данные (видеозаписи, теневые копии) (рис. Контекстное меню события с дополнительными данными 116).

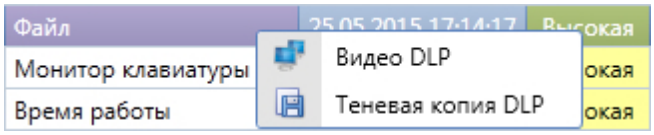


Рисунок 103. Контекстное меню события с дополнительными данными

Просмотр видеозаписей

SoftControl DLP Client сохраняет последовательность снимков экрана клиентского хоста, которая может быть воспроизведена как видеозапись в консоли управления. Для событий типов **файл**, **реестр** и **HTTP** доступен просмотр видеозаписей, если в настройках наблюдаемых объектов выставлена опция **Запись видео**. Вызовите контекстное меню нажатием правой кнопки мыши на событии и выберите пункт **Видео DLP**, чтобы открыть видеозапись (рис. Контекстное меню события с дополнительными данными 116).

В появившемся окне проигрывателя нажмите на кнопку **Загрузить** и управляйте воспроизведением с помощью кнопок (рис. Проигрыватель видеозаписей SoftControl DLP Client 116), предназначение которых приведено в табл. 23.

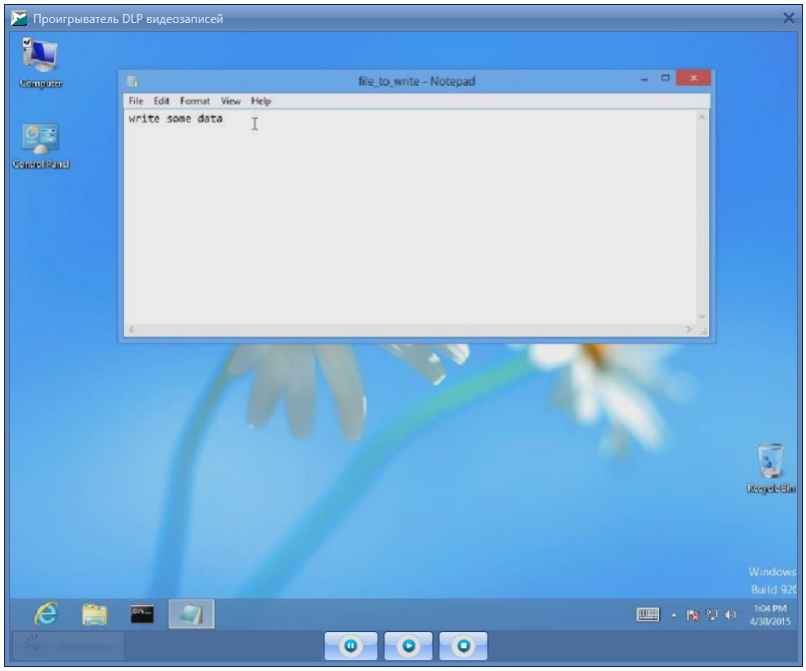


Рисунок 104. Проигрыватель видеозаписей SoftControl DLP Client

Таблица 23. Элементы управления видеопроигрывателя

Кнопка	Название	Описание
	Воспроизвести	Воспроизведение записи.
	Пауза	Пауза воспроизведения.
	Стоп	Остановка воспроизведения.

Для корректной обработки записей серверным компонентом SoftControl Server в ОС Microsoft® Windows® Server 2008 R2 и Microsoft® Windows® Server 2012 / 2012 R2 необходимо предварительно установить дополнительный системный компонент *Возможности рабочего стола* (*Desktop Experience*). Указания по установке даны в приложении 171.

Просмотр теневых копий

Для событий типов **файл** и **реестр** доступен просмотр теневых копий объектов, если в настройках наблюдения для данных объектов выставлена опция **Теневая копия**. Вызовите контекстное меню нажатием правой кнопки мыши на событии, выберите

пункт **Теневая копия DLP** (рис. Контекстное меню события с дополнительными данными[116]) и в появившемся окне **Просмотр теневой копии DLP** нажмите на кнопку **Открыть**, чтобы просмотреть сохранённую копию указанного объекта наблюдения (рис. Теневая копия объекта наблюдения[118]).

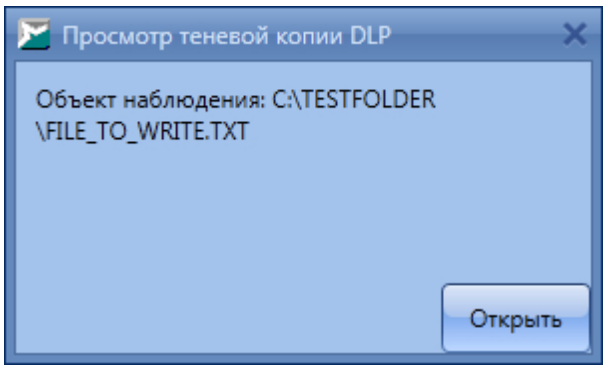


Рисунок 105. Теневая копия объекта наблюдения

4.8.3 Фильтрация событий

Страничное отображение

Информация на вкладке **Лог** отображается в постраничном режиме. Ограничение максимального количества событий на странице задаётся в настройках интерфейса SoftControl Admin Console[28] (по умолчанию – 10 000 событий).

> Не рекомендуется выставлять значение параметра **Размер страницы событий** большим 100 000 событий для предотвращения снижения производительности.

Записи в таблице вкладки упорядочены по страницам в прямом хронологическом порядке, т.е. странице с наибольшим номером соответствует последняя по времени порция событий. При открытии вкладки загружается первая страница. Для навигации по страницам используйте соответствующие кнопки в нижней части вкладки (рис. Навигация по страницам[118]). Переход осуществляется только на соседние страницы.

Рисунок 106. Навигация по страницам

Группировка данных

Информация на вкладке **Лог** может группироваться по всем полям (категориям) для

удобства отображения. Полями (категориями), по которым возможно произвести группировку на дополнительной вкладке **Сканнер**, являются **Путь** (по умолчанию), **Вирус**, **Результат** и **Действие**. Для группировки по категориям перетащите заголовок колонки на панель, расположенную между заголовком таблицы и группой кнопок вкладки (см. рисунки, начиная с Вкладка "Лог" для компонента SoftControl DLP Client 113 и до Теневая копия объекта наблюдения 118 в разделе выше 113). Если группировка производится по нескольким категориям, то приоритет (вложенность категорий) уменьшается слева направо в зависимости от расположения на панели.

Фильтрация с использованием предустановленных фильтров

В SoftControl Admin Console предусмотрены встроенные фильтры для выборки событий.

Чтобы применить предустановленные в программе общие фильтры, откройте меню **Фильтры** и выберите один из вариантов:

- **По умолчанию** – отображение всех типов событий по полям, несущим основную информацию (применяется по умолчанию при открытии вкладки).
- **Полный вид** – отображение всех типов событий по всем возможным полям.
- **Статус** – отображение событий по изменению статуса клиентских приложений.
- **Обновление клиента** – отображение событий по обновлению клиентских приложений.

Чтобы применить предустановленные фильтры, соответствующие типам событий клиентского компонента SoftControl SysWatch, откройте меню **Фильтры** → **Фильтры событий SysWatch** и выберите один из вариантов:

- **Все;**
- **Нарушение политики контроля**;
- **Контроль активности**;
- **Запуск процесса**;
- **Антивирус**;
- **Изменение настроек**;
- **Вход пользователя**;
- **Выход пользователя**;
- **Событие службы**.

Чтобы применить предустановленные фильтры, соответствующие типам событий

клиентского компонента SoftControl DLP Client, откройте меню **Фильтры** → **Фильтры событий DLP** и выберите один из вариантов:

- **Все;**
- **Добавлено устройство;**
- **Вложение;**
- **Файл**;
- **HTTP**;
- **Монитор клавиатуры**;
- **Принтер**;
- **Реестр**;
- **Устройство отсоединено**;
- **Время работы**.

Фильтрация применяется только к записям текущей страницы.

При наличии большого количества событий во время работы фильтра отображается индикатор выполнения. При необходимости процесс можно остановить.

Фильтрация с использованием пользовательских фильтров

Возможно самостоятельно настроить параметры выборки и сохранить их в качестве нестандартного фильтра, который вызывается из меню **Фильтры** → **Пользовательские фильтры**.

Для добавления нового поля в таблицу текущей вкладки нажмите кнопку **Выбрать колонки** и перетащите требуемое поле из окна **Выбор колонок** (рис. Выбор колонок 120) в необходимое место заголовка таблицы. Для удаления существующего поля перетащите его в окно **Выбор колонок**, либо за пределы заголовка таблицы.

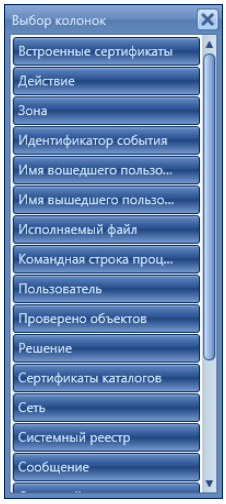


Рисунок 107. Выбор колонок

Для того чтобы отфильтровать выборку по значениям полей, переместите курсор мыши на название поля и нажмите левой кнопкой мыши на появившемся значке ключа, после чего укажите критерий выборки в выпадающем списке (рис. Фильтр по полю 121).

Фильтрацию выборки можно производить по нескольким полям одновременно. В заголовках полей, по которым производится фильтрация, значок ключа отображается постоянно.

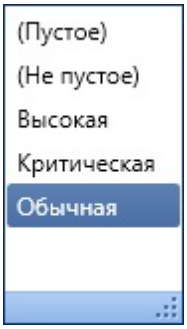


Рисунок 108. Фильтр по полю

В SoftControl Admin Console существует возможность тонкой подстройки параметров выборки с помощью средства **Редактор фильтра**. Если на вкладке **Лог** производится фильтрация по какому-либо из полей, в нижней части вкладки отображается строка параметров фильтра.

Для вызова окна редактора нажмите кнопку **Редактировать фильтр** в правой части строки параметров. Окно редактора показано на рис. Редактор фильтра 121.

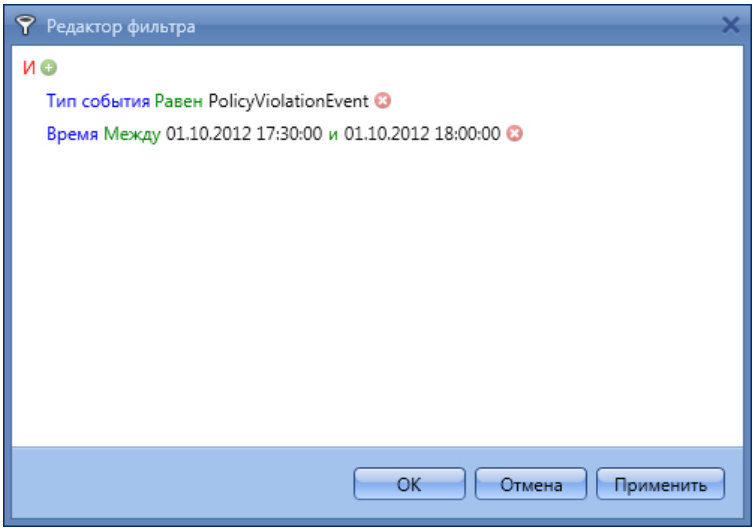


Рисунок 109. Редактор фильтра

В первой строке редактора красным цветом указано логическое условие, по которому объединяются параметры фильтра. Для изменения логического условия нажмите на него левой кнопкой мыши, при этом в выпадающем меню доступны следующие логические операторы:

- И;
- ИЛИ;
- Не И;
- Не ИЛИ.

Для добавления нового параметра фильтра выберите пункт меню **Добавить Условие**, либо нажмите на значок плюса около логического условия. Для добавления параметра фильтра, состоящего из нескольких параметров, объединённых по своему логическому условию, выберите пункт меню **Добавить Группу**. Работа с элементами группы аналогична работе с элементами общего списка. Возможно создание вложенных групп. Для очистки фильтра выберите пункт меню **Очистить всё**. Нажмите **OK**, чтобы сохранить параметры фильтра.

Синтаксис строки параметра фильтра выглядит следующим образом: *<поле, по которому производится фильтрация> <условие> <значение>.* Каждый элемент строки параметра можно изменить, нажав на него. Варианты условия автоматически определяются исходя из типа поля.

Для упорядочивания данных в таблицах вкладок по определённым полям нажмите

левой кнопкой мыши на требуемом поле и одиночным нажатием задайте направление сортировки, которое индицируется стрелкой правее названия поля.

Чтобы сохранить полученную с параметрами пользователя выборку для дальнейшего использования, нажмите на кнопку **Сохранить настройки вида**, введите имя фильтра в появившемся окне и нажмите **OK** (рис. Сохранение фильтра 123).

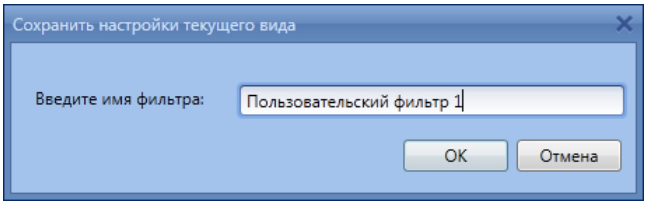


Рисунок 110. Сохранение фильтра

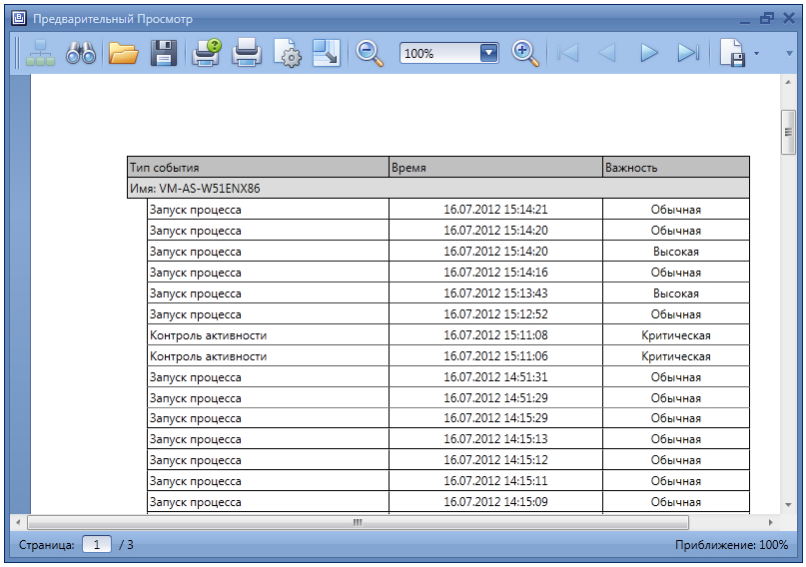
Фильтрация применяется только к записям текущей страницы.

При наличии большого количества событий во время работы фильтра отображается индикатор выполнения. При необходимости процесс можно остановить.

4.8.4 Печать и экспорт в файлы отчётов

В SoftControl Admin Console существует несколько возможностей экспорта накопленной информации в отчётах клиентских приложений.

Для вывода отчёта на печать произведите выборку с помощью необходимых фильтров 118 и нажмите на кнопку **Печать**. В открывшемся окне предварительного просмотра можно задать **Настройки страницы** и **Масштаб** с помощью соответствующих кнопок (рис. Предварительный просмотр печати 123).



Тип события	Время	Важность
Имя: VM-AS-W51ENX86		
Запуск процесса	16.07.2012 15:14:21	Обычная
Запуск процесса	16.07.2012 15:14:20	Обычная
Запуск процесса	16.07.2012 15:14:20	Высокая
Запуск процесса	16.07.2012 15:14:16	Обычная
Запуск процесса	16.07.2012 15:13:43	Высокая
Запуск процесса	16.07.2012 15:12:52	Обычная
Контроль активности	16.07.2012 15:11:08	Критическая
Контроль активности	16.07.2012 15:11:06	Критическая
Запуск процесса	16.07.2012 14:51:31	Обычная
Запуск процесса	16.07.2012 14:51:29	Обычная
Запуск процесса	16.07.2012 14:15:29	Обычная
Запуск процесса	16.07.2012 14:15:13	Обычная
Запуск процесса	16.07.2012 14:15:12	Обычная
Запуск процесса	16.07.2012 14:15:11	Обычная
Запуск процесса	16.07.2012 14:15:09	Обычная

Рисунок 111. Предварительный просмотр печати

Нажмите на кнопку **Печать** для вывода стандартного окна настроек принтера, либо на кнопку **Быстрая печать** для мгновенной отправки на печать с установками принтера по умолчанию.

Для сохранения отчёта в таблицу Excel произведите выборку с помощью необходимых фильтров [118] и нажмите на кнопку **Экспорт в Excel**. В диалоговом окне сохранения укажите место для сохранения отчёта и его имя, после чего нажмите на кнопку **Сохранить** (Save).

4.9 Оповещения о событиях

Оповещения (нотификации) о событиях, регистрируемых в Сервисном Центре, позволяют администратору оперативно реагировать на возникающие угрозы, даже в случае отсутствия за штатной рабочей станцией с установленной консолью управления SoftControl Admin Console.

Первоначально необходимо задать контактные данные [125] получателей оповещений, после чего настроить параметры отправки [126].

4.9.1 Контакты

На вкладке **Контакты** производится задание адресатов – получателей нотификаций (рис. Вкладка "Контакты" 125).

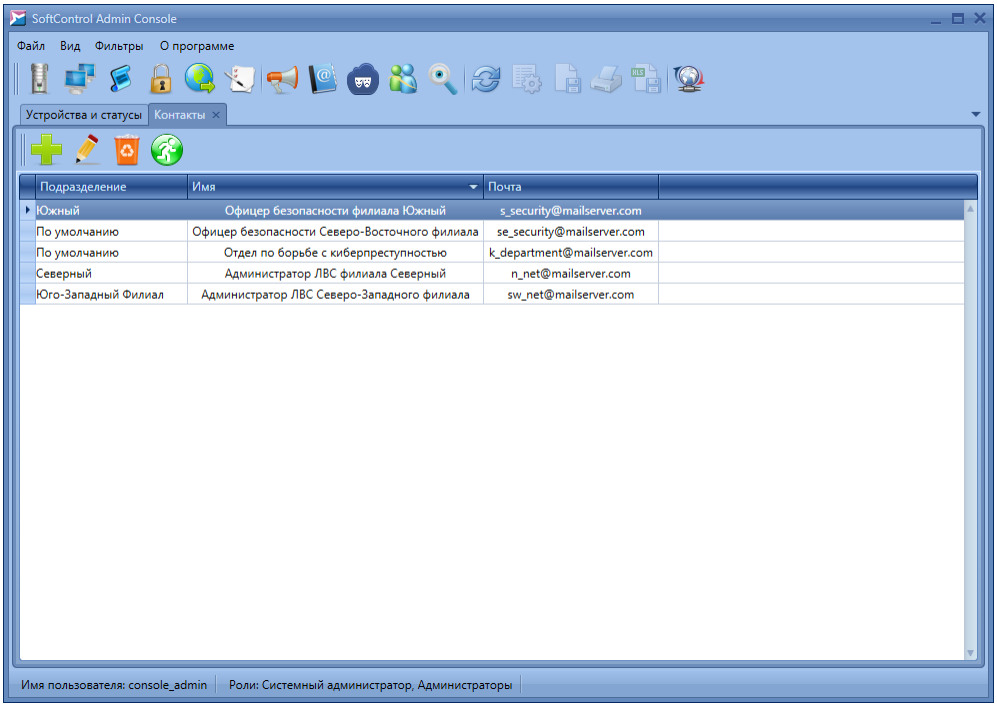


Рисунок 112. Вкладка "Контакты"

Основные операции с контактами осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 24.

Таблица 24. Элементы управления вкладки "Контакты"

Кнопка	Название	Описание
	Создать	Создание нового контакта.
	Правка	Редактирование свойств выбранного контакта.
	Удалить	Удаление выбранных контактов.
	Переместить	Перемещение выбранного контакта в другое подразделение.

Перечень полей вкладки приведён в табл. 25.

Таблица 25. Поля вкладки "Контакты"

Поле	Описание
Подразделение	Подразделение, к которому принадлежит данный контакт.
Имя	Имя получателя.
Почта	Адрес электронного почтового ящика получателя.

Чтобы добавить нового получателя, нажмите на кнопку **Создать** (рис. Вкладка "Контакты" 125). В появившемся окне укажите данные получателя в полях **Имя** и **Электронная почта** и нажмите на кнопку **Применить** (рис. Добавление контакта 126).

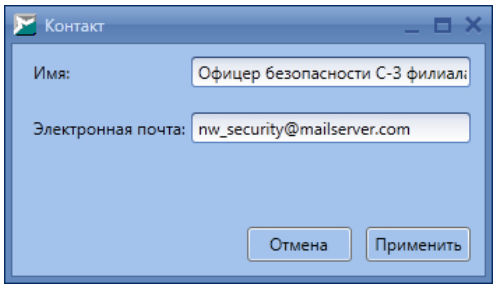


Рисунок 113. Добавление контакта

Для правки и удаления контактов воспользуйтесь соответствующими кнопками.

4.9.2 Нотификации

Вкладка **Нотификации** предназначена для настройки параметров отправки оповещений о событиях посредством электронной почты (рис. Вкладка "Нотификации" 126).

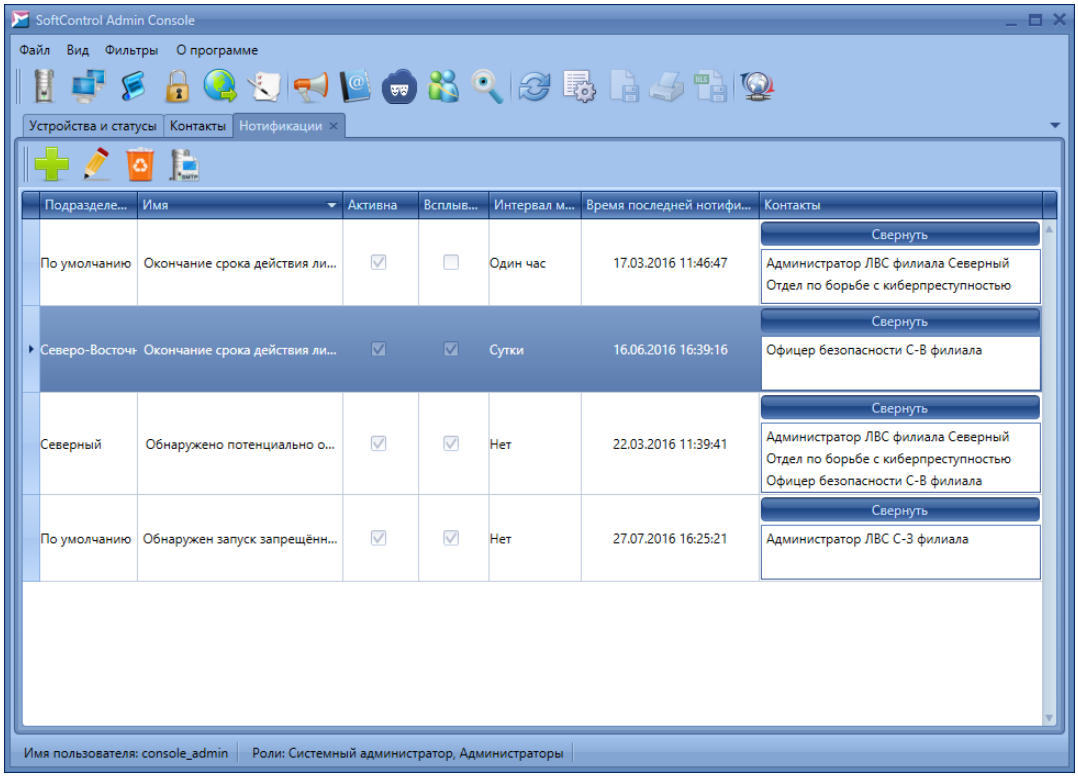


Рисунок 114. Вкладка "Нотификации"

Основные операции с нотификациями осуществляются с помощью графических кнопок

вкладки, предназначение которых приведено в табл. 26.

Таблица 26. Элементы управления вкладки "Нотификации"

Кнопка	Название	Описание
	Создать	Создание новой нотификации.
	Редактировать	Редактирование выбранной нотификации.
	Удалить	Удаление выбранных нотификаций.
	SMTP	Настройка SMTP-сервера.

Перечень полей вкладки приведён в табл. 27.

Таблица 27. Поля вкладки "Нотификации"

Поле	Описание
Подразделение	Подразделение, к которому относится данная нотификация.
Имя	Наименование нотификации.
Активна	Флажок состояния нотификации.
Всплывающее сообщение	Флажок, указывающий отображается ли всплывающее уведомление при отправке нотификации.
Интервал между отправками	Минимальный временной интервал после отправки предыдущей нотификации, по истечении которого возможна отправка следующей.
Время последней нотификации	Время отправки последней нотификации.
Правило	Условия срабатывания отправки нотификации.
Контакты	Список адресатов электронного письма с нотификацией.

Основные действия, выполняемые на данной вкладке:

Настройка SMTP-сервера

Для работы нотификаций необходимо предварительно настроить параметры сервера исходящей почты по протоколу SMTP, для этого нажмите на кнопку **SMTP** (рис. Вкладка "Нотификации" 126).

В окне **Настройка почтового сервера** введите в поле **Почтовый сервер** адрес почтового сервера, с электронного ящика которого предполагается отправка нотификаций, а также **Номер порта** для отправки (рис. Настройка почтового сервера 128). В полях **Логин**, **Пароль** и **Почтовый ящик** введите данные учётной записи и адрес почтового ящика, с которого предполагается отправка нотификаций. Установите флажок **Использовать SSL** для криптографической защиты при передаче данных.

Чтобы проверить работоспособность введённых настроек, нажмите на кнопку **Отправить тестовое письмо**.

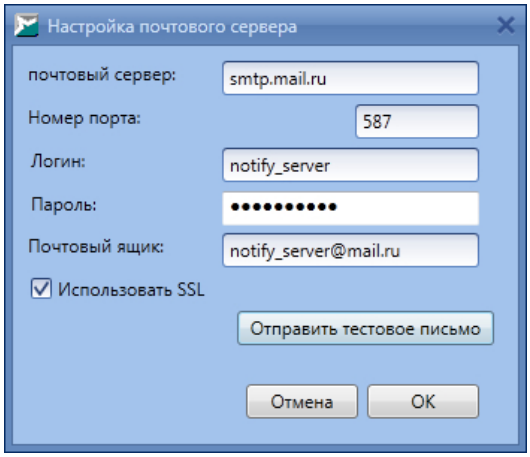


Рисунок 115. Настройка почтового сервера

Нажмите на кнопку **OK** для применения настроек.

Создание нотификации

Чтобы добавить новую нотификацию, нажмите на кнопку **Создать** (рис. Вкладка "Нотификации" 126).

В появившемся окне на вкладке **Общие** укажите **Имя** нотификации, выберите минимальный **Интервал между отправками** в выпадающем списке, введите **Тему** письма и установите флажок **Активировать** (рис. Общие параметры нотификации 128).

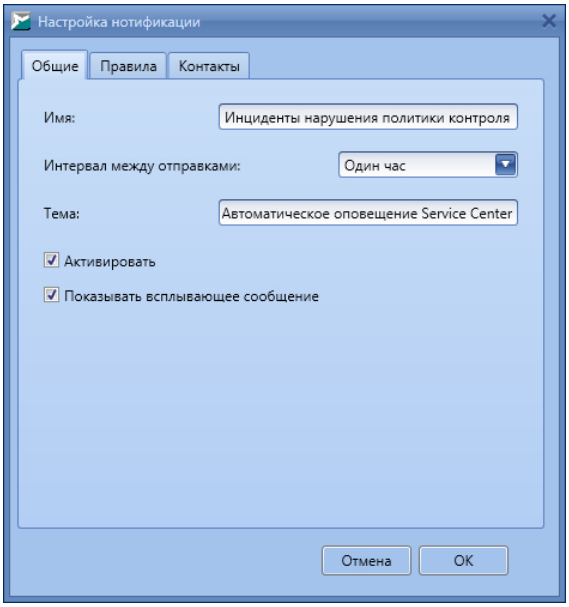


Рисунок 116. Общие параметры нотификации

Чтобы **Показывать всплывающее сообщение** при отправке нотификации, установите соответствующий флажок. В этом случае после отправки нотификации будет отображаться всплывающее уведомление с заголовком оповещения (рис. Всплывающее уведомление[129]).

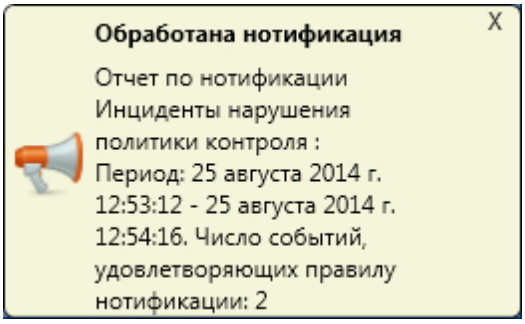


Рисунок 117. Всплывающее уведомление

На вкладке **Правила** выберите условие, при наступлении которого будет производиться отправка нотификации (рис. Условия срабатывания отправки нотификации[129]):

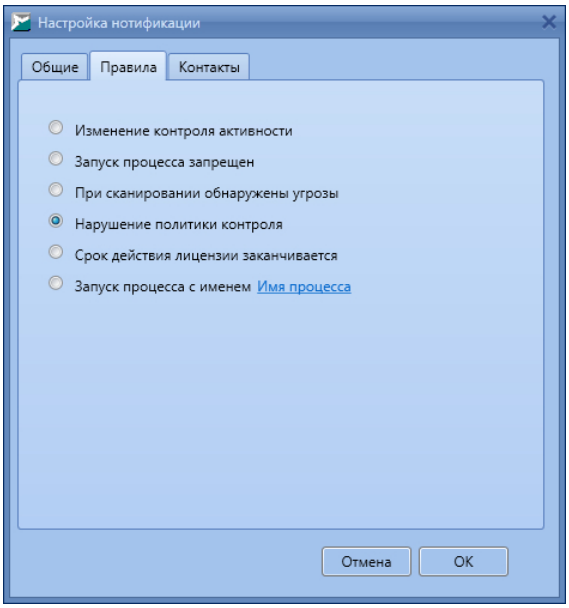


Рисунок 118. Условия срабатывания отправки нотификации

- **Изменение контроля активности**:

  изменение статусов контроля активности компонента SoftControl SysWatch по любой из областей.

- **Запуск процесса запрещен**:

  регистрация события типа "запуск процесса" компонентом SoftControl SysWatch с

решением "запрещено".

○ **При сканировании обнаружены угрозы**:

обнаружение вредоносного кода в процессе антивирусной проверки компонентом SoftControl SysWatch.

○ **Нарушение политики контроля**:

регистрация события типа "нарушение политики контроля" компонентом SoftControl SysWatch.

○ **Срок действия лицензии заканчивается**:

до конца срока действия лицензионного ключа клиентского компонента остаётся меньше 10 дней.

Рекомендуется устанавливать значение параметра **Интервал между отправками** для данной нотификации не менее 4 часов.

○ **Запуск процесса с именем**:

регистрация события типа "запуск процесса" с именем, заданным по ссылке **Имя процесса**, компонентом SoftControl SysWatch.

На вкладке **Контакты** отметьте адресатов отправки нотификации (рис. Выбор получателей нотификации 130).

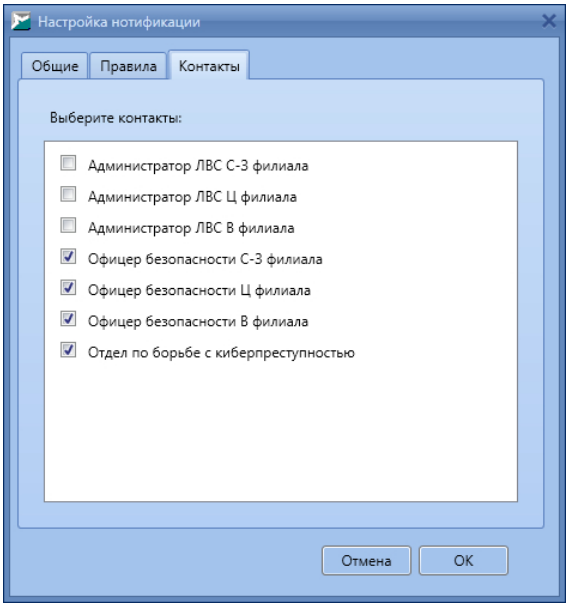


Рисунок 119. Выбор получателей нотификации

Нажмите на кнопку **OK**, чтобы подтвердить создание нотификации.

Изменение свойств нотификации

Чтобы изменить свойства нотификации, выберите её и выполните одно из следующих действий:

- нажмите на кнопку **Редактировать** в группе кнопок вкладки (рис. Вкладка "Нотификации"[126]);
- дважды нажмите левой кнопки мыши на нотификации.

В появившемся окне измените необходимые параметры аналогично работе с новой нотификацией (рис. Общие параметры нотификации[128], Условия срабатывания отправки нотификации[129], Выбор получателей нотификации[130]).

Нажмите на кнопку **OK**, чтобы подтвердить изменения.

Отключение и удаление нотификации

Если необходимо отключить получение нотификации без её удаления из списка, вызовите окно редактирования свойств, сбросьте флажок **Активировать** на вкладке **Общие** и нажмите на кнопку **OK** (рис. Общие параметры нотификации[128]).

Для удаления нотификации выберите её, нажмите на кнопку **Удалить** (рис. Вкладка "Нотификации"[126]) и подтвердите удаление в диалоговом окне.

5. Обновление компонентов СИБ

SoftControl Service Center предоставляет возможность централизованного обновления всех компонентов системы с автоматически развёртываемого локального сервера. Вкладка **Обновления** позволяет произвести настройку и просмотреть историю обновлений (рис. Вкладка "Обновления" для программных модулей 132, Вкладка "Обновления" для антивирусных баз 135).

В верхней части вкладки представлено две категории настроек для обновления соответствующих компонентов:

- Программные модули 132;
- Антивирусные базы 135.

В нижней части вкладки представлена история обновлений, содержащая список выполняемых операций. Перечень полей списка приведён в табл. 28.

Таблица 28. Поля списка истории обновлений

Поле	Описание
Последняя проверка	Дата и время последней проверки наличия обновлений.
Последнее обновление	Дата и время последней установки обновлений.
Компонент	Название обновляемого компонента.
Статус обновления	Состояние обновления: • **Обновление не требуется**; • **Доступно обновление**; • **Обновление загружено**; • **Обновление установлено**; • **Ошибка обновления**.
Размер обновления	Размер обновления в байтах.
Актуальная версия	Текущая версия установленного компонента.
Новая версия	Версия компонента, доступная к обновлению.
Детали	Дополнительная информация.

5.1 Настройка обновления программных модулей

Данная категория настроек позволяет настраивать и управлять обновлением программных модулей компонентов SoftControl Service Center, а также ретрансляцией обновлений программных модулей клиентских компонентов SoftControl SysWatch и SoftControl DLP Client с внешних (Интернет) серверов (рис. Вкладка "Обновления" для программных модулей 132).

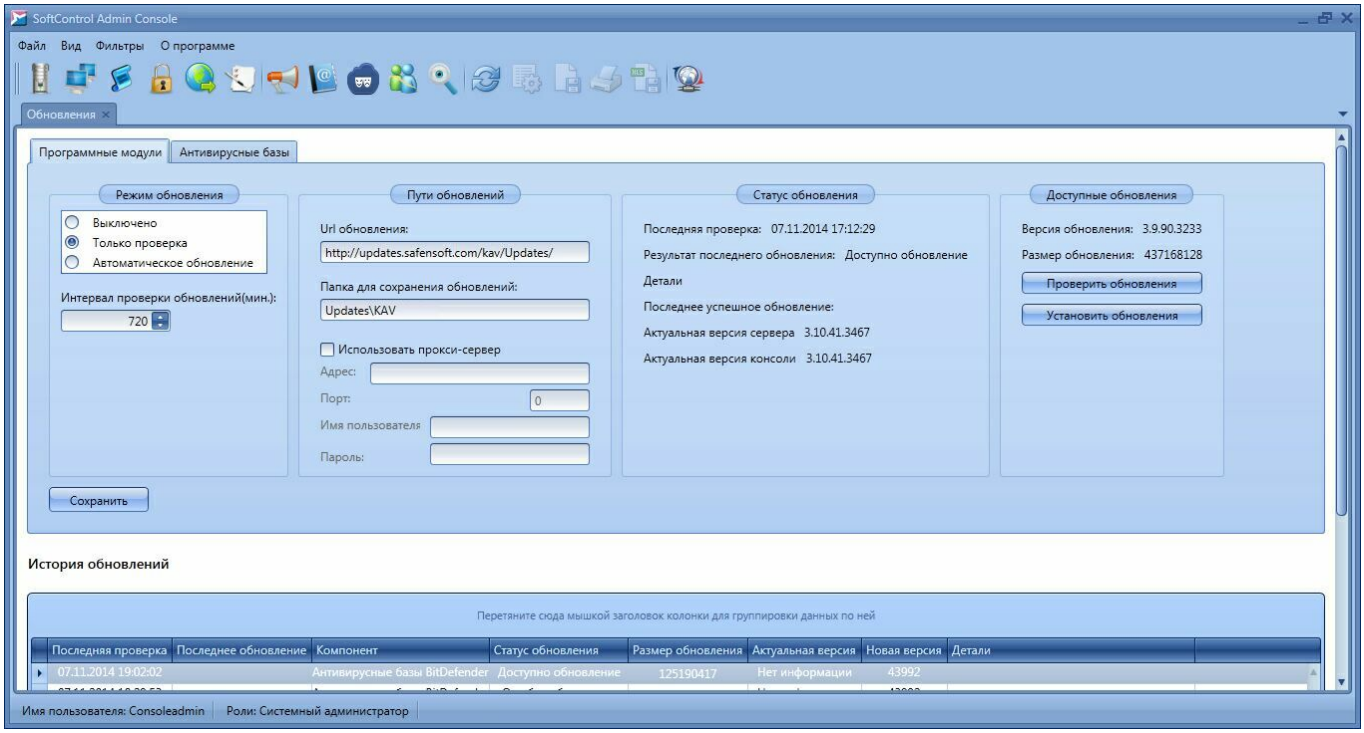


Рисунок 120. Вкладка "Обновления" для программных модулей

Настройка режима обновления

В секции **Режим обновления** возможен выбор трех режимов работы:

- **Выключено**:

  Обновление в автоматическом режиме отключено.

- **Только проверка**:

  SoftControl Service Center автоматически проверяет наличие обновлений на внешних серверах с периодичностью, указанной в счетчике **Интервал проверки обновлений(мин.)**, но не загружает и не устанавливает их.

- **Автоматическое обновление**:

  SoftControl Service Center автоматически проверяет наличие обновлений на внешних серверах с периодичностью, указанной в счетчике **Интервал проверки обновлений(мин.)** и в случае нахождения более новых версий, чем установленные, происходит ретрансляция пакетов обновлений на сервер. Если найдена новая версия SoftControl Service Center, по окончании загрузки установочных пакетов происходит автоматическое обновление компонентов SoftControl Server и SoftControl Admin Console в фоновом режиме на сервере.

При отсутствии доступа в Интернет или в случае возникновения проблем в процессе автоматического обновления, возможно обновление SoftControl

Service Center в ручном режиме[138] при наличии установочного пакета требуемой версии.

Обновление клиентских компонентов[141] осуществляется с созданного локального «зеркала».

Настройка путей обновления и параметров прокси-сервера

В секции **Пути обновления** задаются следующие параметры:

- **Url обновления**:

  Ссылка на внешний сервер, по которой SoftControl Service Center проверяет наличие обновлений.
- **Папка для сохранения обновлений**:

  Путь сохранения пакетов обновления с внешних серверов относительно директории `C:\ProgramData\SoftControl`.

Установите флажок **Использовать прокси-сервер**, если соединение с внешними серверами требуется осуществлять через прокси-сервер. В этом случае задайте его параметры:

- **Адрес**:

  IP-адрес или NetBIOS-имя хоста прокси-сервера.
- **Порт**:

  Номер порта для связи с прокси-сервером (если не указан – используется порт *80* по умолчанию).
- **Имя пользователя**:

  Имя пользователя для аутентификации на прокси-сервере.
- **Пароль**:

  Пароль для аутентификации на прокси-сервере.

Поддерживается базовый (Basic) тип авторизации. Если аутентификация на прокси-сервере не требуется, то поля **Имя пользователя** и **Пароль** следует оставлять пустыми.

Проверка и обновление по запросу

В секции **Доступные обновления** возможно выполнение операций по запросу с

помощью следующих кнопок:

- **Проверить обновления**:

  Проверка наличия обновлений программных модулей. В случае обнаружения обновлений отображается **Версия обновления** и **Размер обновления** (в байтах).
- **Установить обновления** (для случая, когда SoftControl Server и SoftControl Admin Console установлены на одном компьютере):

  Проверка и, в случае обнаружения, ретрансляция пакетов обновлений с внешних серверов, установка обновлений SoftControl Server и SoftControl Admin Console.
- **Обновить сервер** (для случая, когда SoftControl Server и SoftControl Admin Console установлены на разных компьютерах):

  Проверка и, в случае обнаружения, ретрансляция пакетов обновлений с внешних серверов, установка обновлений серверного компонента (SoftControl Server).
- **Обновить консоль** (для случая, когда SoftControl Server и SoftControl Admin Console установлены на разных компьютерах):

  Проверка и, в случае обнаружения, установка обновлений консоли управления (SoftControl Admin Console).

После обновления программных модулей настройки SoftControl Server и SoftControl Admin Console, а также пользовательские фильтры SoftControl Admin Console сохраняются. Накопленные события в SoftControl Admin Console хранятся в БД, поэтому при обновлении не затрагиваются.

В секции **Статус обновления** доступна информация по текущей версии и последним проведенным операциям проверки и установки обновлений.

Для применения изменённых установок нажмите на кнопку **Сохранить**.

5.2 Настройка обновления антивирусных баз

Данная категория настроек позволяет настраивать и управлять ретрансляцией антивирусных баз клиентского компонента SoftControl SysWatch с внешних (Интернет) серверов (рис. Вкладка "Обновления" для антивирусных баз 135).

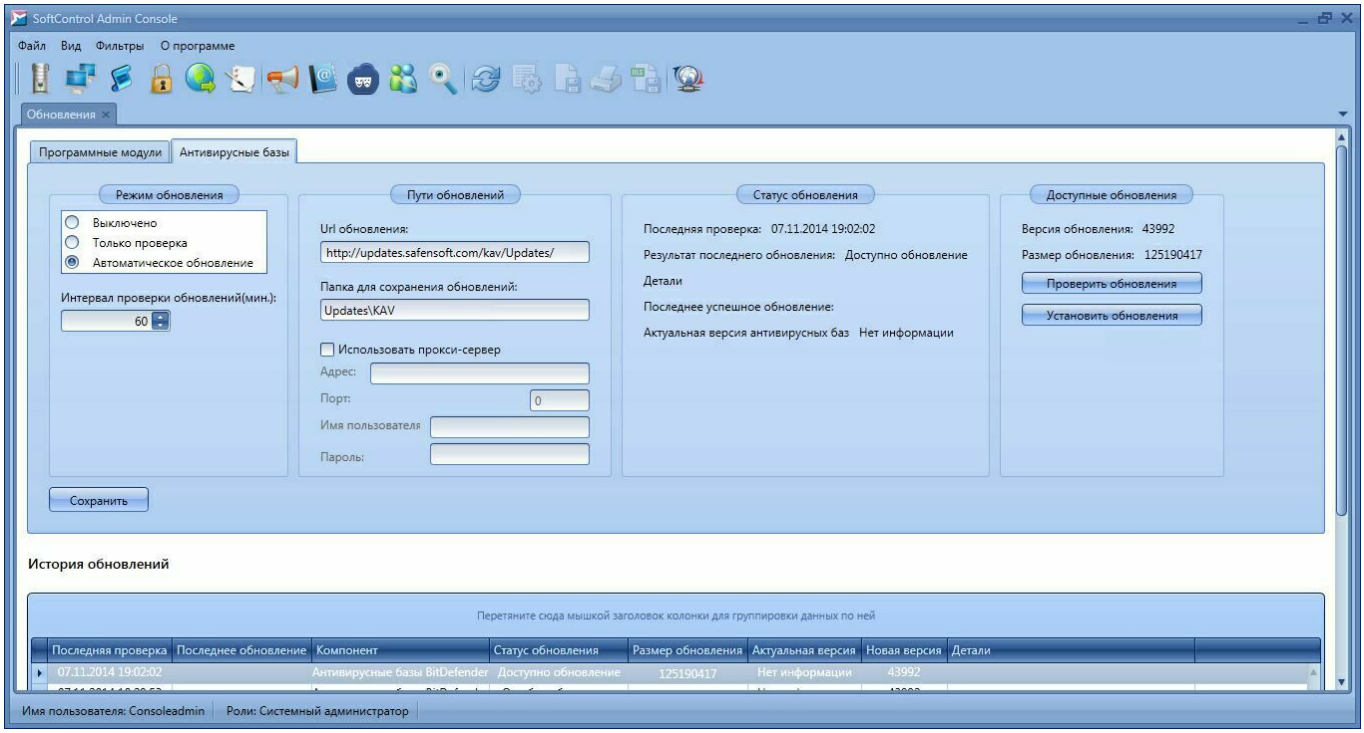


Рисунок 121. Вкладка "Обновления" для антивирусных баз

Настройка режима обновления

В секции **Режим обновления** возможен выбор трех режимов работы:

- **Выключено**:

  Обновление в автоматическом режиме отключено.

- **Только проверка**:

  SoftControl Service Center автоматически проверяет наличие обновлений на внешних серверах с периодичностью, указанной в счетчике **Интервал проверки обновлений(мин.)**, но не загружает их.

- **Автоматическое обновление**:

  SoftControl Service Center автоматически проверяет наличие обновлений на внешних серверах с периодичностью, указанной в счетчике **Интервал проверки обновлений(мин.)** и в случае нахождения более новых версий, чем установленные, происходит ретрансляция обновлений баз на сервер. Обновление антивирусных баз осуществляется в рамках обновления клиентского компонента SoftControl SysWatch [141] с созданного локального «зеркала».

Настройка путей обновления и параметров прокси-сервера

В секции **Пути обновления** задаются следующие параметры:

- **Url обновления**:

  Ссылка на внешний сервер, по которой SoftControl Service Center проверяет наличие обновлений. Ссылки для разных антивирусных баз описаны в табл. 29.

Таблица 29. Адреса обновлений антивирусных баз

Название	Адрес	Папка для сохранения
Антивирусные базы Kaspersky Anti-virus	http://updates.safensoft.com/kav/	Updates\KAV
Антивирусные базы Avira	http://updates.safensoft.com/av4/	Updates\AV4

- **Папка для сохранения обновлений**:

  Путь сохранения пакетов обновления с внешних серверов относительно директории `C:\ProgramData\SoftControl`. Папки для разных антивирусных баз описаны в табл. 29.

Установите флажок **Использовать прокси-сервер**, если соединение с внешними серверами требуется осуществлять через прокси-сервер. В этом случае задайте его параметры:

- **Адрес**:

  IP-адрес или NetBIOS-имя хоста прокси-сервера.
- **Порт**:

  Номер порта для связи с прокси-сервером (если не указан – используется порт *80* по умолчанию).
- **Имя пользователя**:

  Имя пользователя для аутентификации на прокси-сервере.
- **Пароль**:

  Пароль для аутентификации на прокси-сервере.

Поддерживается базовый (Basic) тип авторизации. Если аутентификация на прокси-сервере не требуется, то поля **Имя пользователя** и **Пароль** следует оставлять пустыми.

Проверка и обновление по запросу

В секции **Доступные обновления** возможно выполнение операций по запросу с помощью следующих кнопок:

- **Проверить обновления** (кроме случая баз Kaspersky Anti-virus):

  Проверка наличия обновлений антивирусных баз. В случае обнаружения обновлений отображается **Версия обновления** и **Размер обновления** (в байтах).
- **Установить обновления**:

  Проверка и, в случае обнаружения, ретрансляция антивирусных баз с внешних серверов.

По умолчанию в поставку SoftControl Service Center входит пробный лицензионный ключ к базам Kaspersky Anti-virus. После истечения срока действия пробного ключа обновление баз Kaspersky Anti-virus становится невозможным. Поэтому приобретите коммерческую лицензию KAV и поместите полученный файл лицензии с расширением *.key* в следующий каталог компьютера с установленным компонентом SoftControl Server:

`<каталог установки SoftControl Server>\Tools\Updates\Plugins\KAV\`

В секции **Статус обновления** доступна информация по текущей версии и последним проведенным операциям проверки и установки обновлений.

Для применения изменённых установок нажмите на кнопку **Сохранить**.

5.3 Обновление SoftControl Server и SoftControl Admin Console в ручном режиме

1) Запустите установочный пакет *Service.Center.msi* версии, на которую необходимо произвести обновление.
2) В окне **Установка SoftControl Service Center** нажмите на кнопку **Далее** (рис. Запуск программы обновления 138).

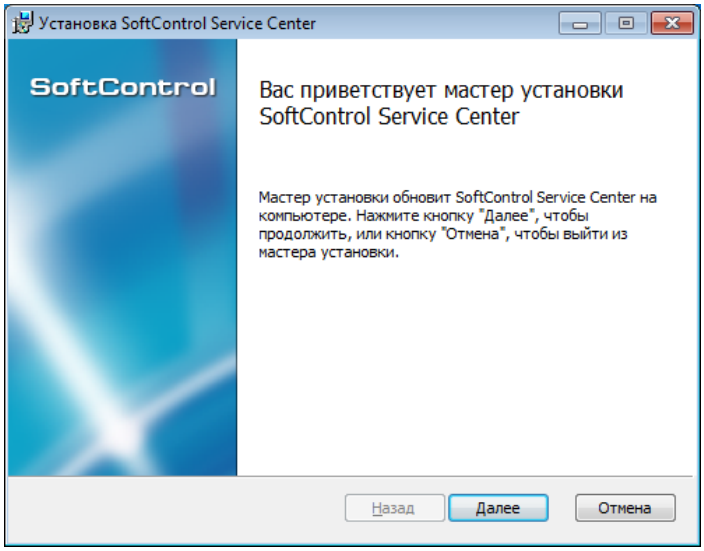


Рисунок 122. Запуск программы обновления

3) В случае вашего согласия, отметьте опцию **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее** (рис. Лицензионное соглашение 139).

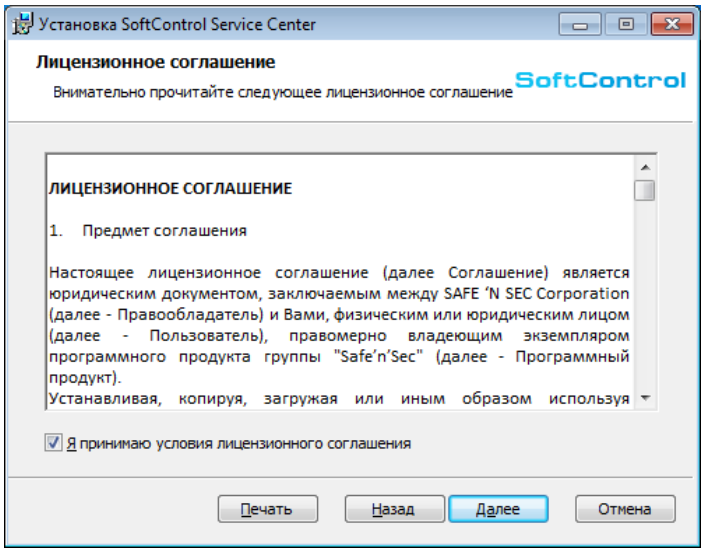


Рисунок 123. Лицензионное соглашение

4) Нажмите на кнопку **Обновить** (рис. Готовность к обновлению 139).

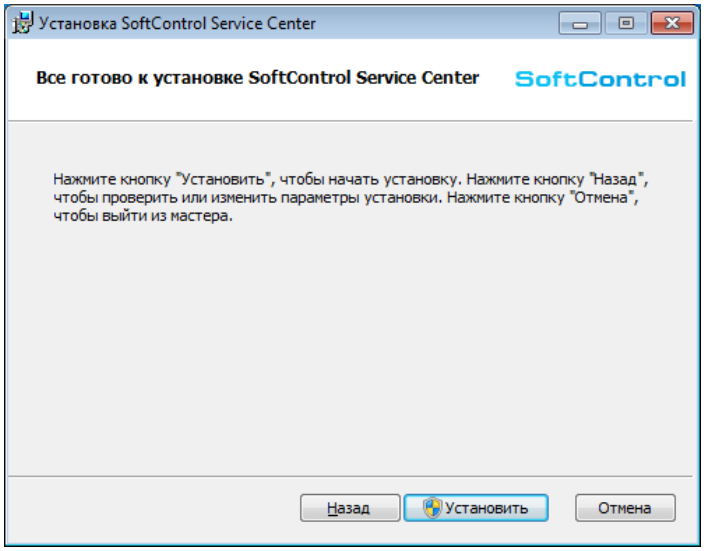


Рисунок 124. Готовность к обновлению

5) Дождитесь окончания процесса обновления (рис. Процесс обновления [140]).

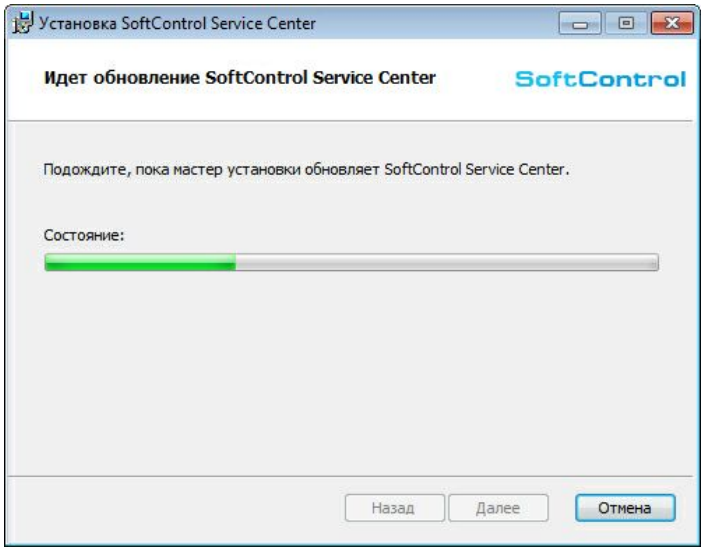


Рисунок 125. Процесс обновления

6) После появления сообщения *Установка SoftControl Service Center завершена* нажмите на кнопку **Готово** (рис. Завершение обновления [140]).

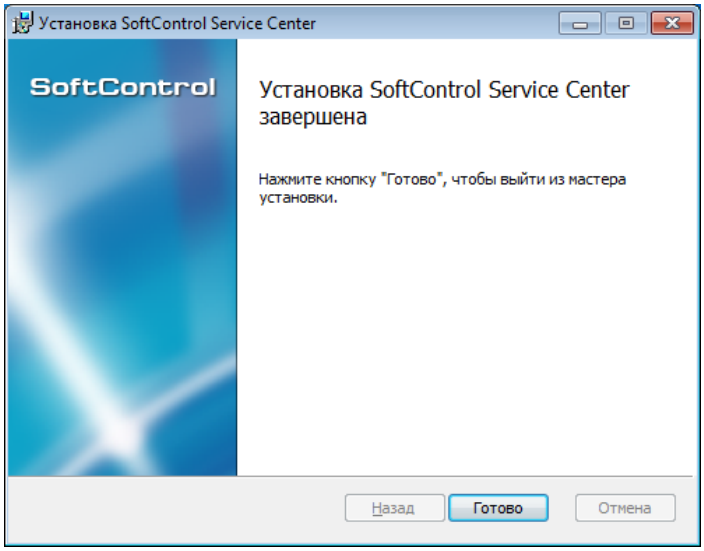


Рисунок 126. Завершение обновления

5.4 Обновление клиентских компонентов

После ретрансляции обновлений с внешних серверов клиентские компоненты могут быть обновлены с SoftControl Service Center следующими способами:

- После подключения к Сервисному Центру SoftControl SysWatch и SoftControl DLP Client автоматически переключаются в режим обновлений с него. Обновление компонентов производится по запросу посредством создания соответствующей задачи[104] или по расписанию, если оно настроено для SoftControl SysWatch[66] / SoftControl DLP Client[97].
- Находясь в автономном режиме работы, SoftControl SysWatch также может быть обновлен с Сервисного Центра. Для этого в настройках источников обновления SoftControl SysWatch через интернет замените предустановленные адреса на соответствующие табл. 30 локальные адреса для необходимых компонентов. Порт связи с сервером по умолчанию – *8088*. После применения указанных настроек обновление можно произвести по запросу через ГИП.

Таблица 30. Адреса обновлений с SoftControl Service Center

Компонент	Описание	Адрес
Core	Программные модули	http://<IP-адрес сервера>:<порт связи с сервером>/api/updates/SNS
AV_AV1	Антивирусные базы Bitdefender	http://<IP-адрес сервера>:<порт связи с сервером>/api/updates/BIT
AV_KAV	Антивирусные базы Kaspersky Anti-virus	http://<IP-адрес сервера>:<порт связи с сервером>/api/updates/KAV
AV_AV3	Антивирусные базы	http://<IP-адрес сервера>:<порт связи с сервером>/api/

Компонент	Описание	Адрес
	Commtouch Anti-virus	updates/CT
AV-AV4	Антивирусные базы Avira	http://<IP-адрес сервера>:<порт связи с сервером>/api/updates/AV4

6. Удаление компонентов SoftControl Service Center

Удаление SoftControl Server и SoftControl Admin Console: в Панели управления Windows в разделе **Программы** (Programs) → **Программы и компоненты** (Programs and Features) выберите *SoftControl Service Center* и нажмите на кнопку **Удалить** (Uninstall).

Удаление одного из компонентов:

1) В Панели управления Windows в разделе **Программы** (Programs) → **Программы и компоненты** (Programs and Features) выберите *SoftControl Service Center* и нажмите на кнопку **Изменить** (Change).
2) В окне **Установка SoftControl Service Center** нажмите на кнопку **Далее** (рис. Запуск программы удаления 143).

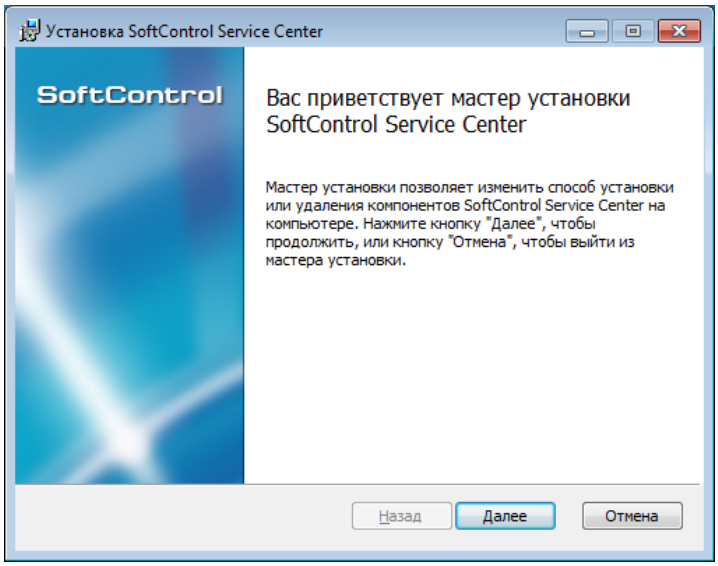


Рисунок 127. Запуск программы удаления

3) Выберите операцию **Изменить** (рис. Типы операций 143).
4) Выберите компонент для удаления (рис. Выбор компонентов для удаления 144): нажмите на пиктограмму компонента и в выпадающем меню выберите опцию **Компонент будет полностью недоступен** (рис. Опции установки компонента 144). После того как все установки завершены, нажмите на кнопку **Далее**.

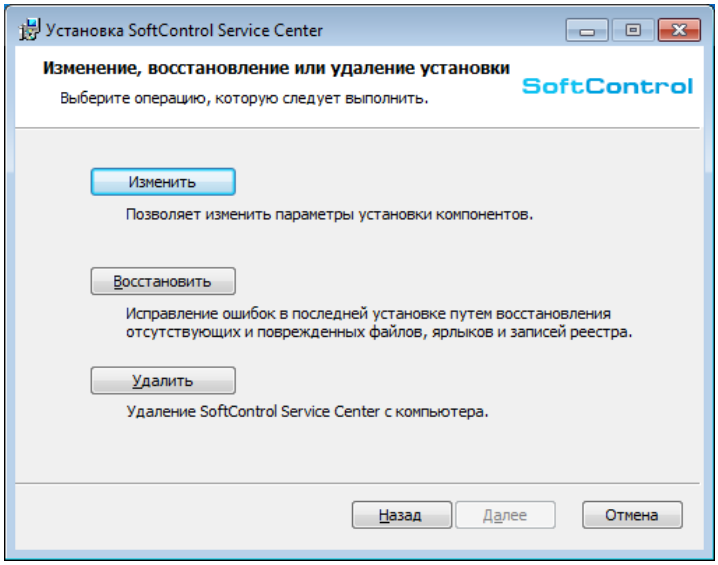


Рисунок 128. Типы операций

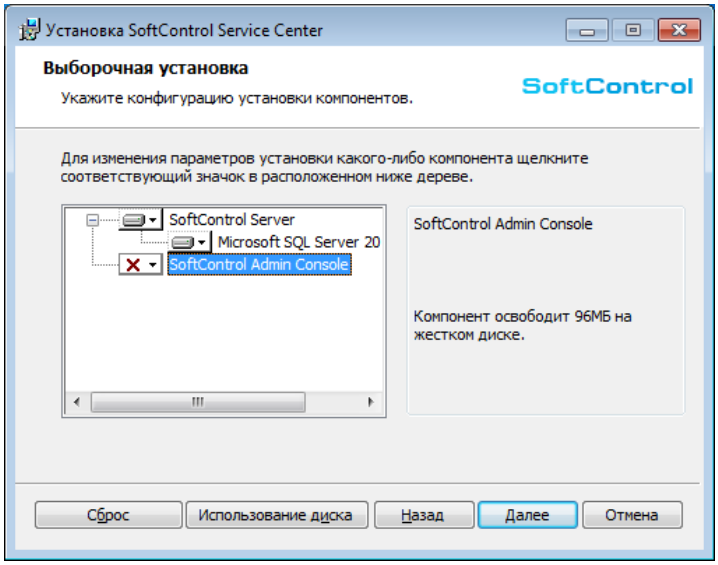


Рисунок 129. Выбор компонентов для удаления

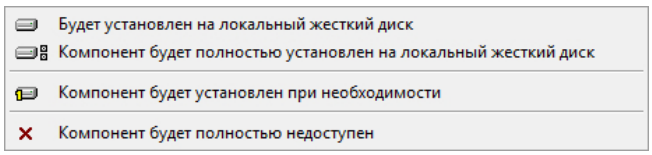


Рисунок 130. Опции установки компонента

5) Нажмите на кнопку **Изменить** (рис. Готовность к удалению 144).

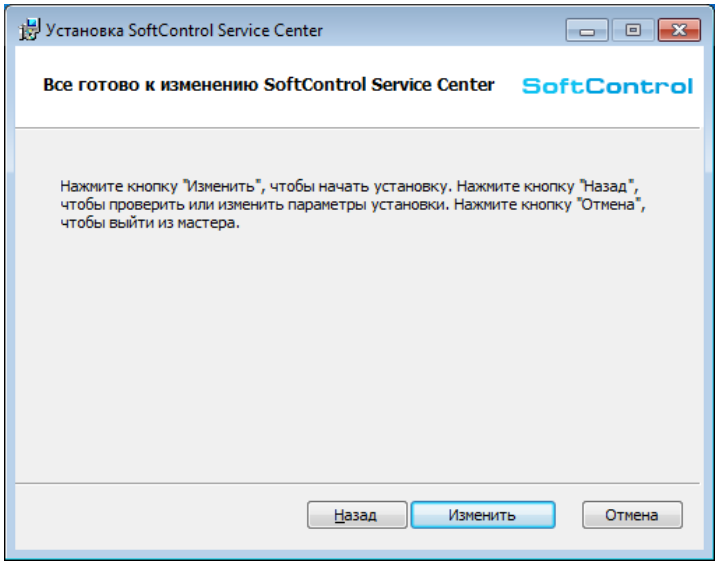


Рисунок 131. Готовность к удалению

6) Дождитесь окончания процесса удаления (рис. Процесс удаления 145).

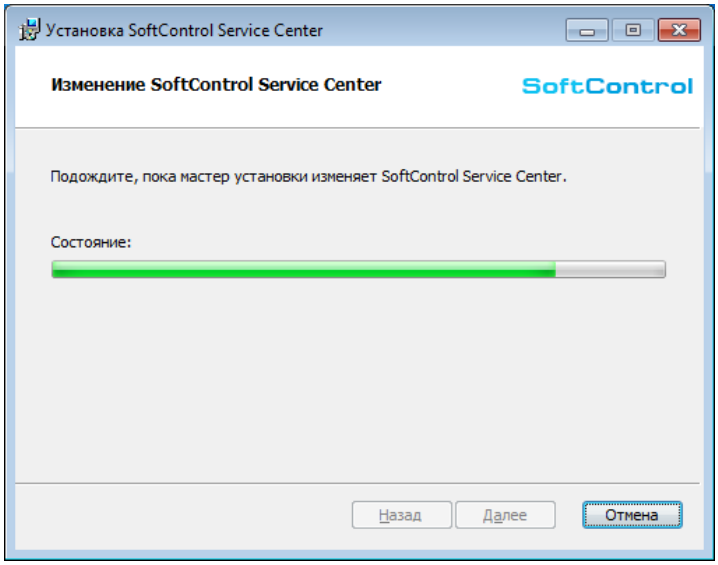


Рисунок 132. Процесс удаления

7) После появления сообщения *Установка SoftControl Service Center завершена* нажмите на кнопку **Готово** (рис. Завершение удаления 145).

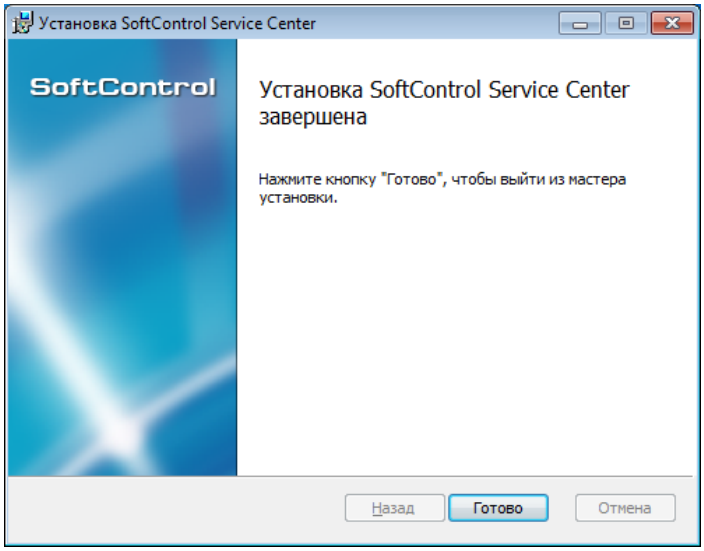


Рисунок 133. Завершение удаления

В случае, если SoftControl Server был установлен со встроенной СУБД, удаление Microsoft® SQL Server® 2014 Express SP1 необходимо произвести вручную. Для этого выполните удаление следующих элементов СУБД стандартными средствами Windows:

- *Microsoft SQL Server 2014*;
- *Microsoft SQL Server 2012 Native Client*;
- *Microsoft SQL Server 2014 Setup (English)*;
- *Microsoft SQL Server 2008 Setup Support Files*;
- *Microsoft SQL Server 2014 Transact-SQL ScriptDom*.

7. Дополнительная информация

7.1 О сертификатах сервера

В настоящем разделе рассматриваются некоторые важные аспекты криптографической защиты канала связи между Сервисным Центром и клиентскими приложениями (далее – «клиентами»).

Для взаимодействия между серверным компонентом SoftControl Server и клиентами в SoftControl Service Center используется протокол HTTPS. Все данные между сервером и конечной точкой передаются в зашифрованном виде по защищённому каналу, при этом для авторизации клиентов используются сертификаты стандарта X.509.

В процессе работы SoftControl Server генерирует следующие виды сертификатов:

- **Корневой** – данный сертификат является сертификатом удостоверяющего центра в рамках СИБ на основе Сервисного Центра и помещается в хранилище Windows. Все остальные виды сертификатов продукта подписаны корневым сертификатом, что является одним из критериев их достоверности.
- **Серверный** – сертификат серверной стороны, используемый для взаимодействия с клиентами и помещаемый в хранилище Windows.
- **Общий клиентский** – сертификат клиентской стороны, используемый для регистрации клиентов на сервере. Данный сертификат является общим для всех новых клиентов и предназначен только для подачи ими первого запроса на сервер. Сертификат встроен в зашифрованный файл клиентских настроек[24], применяемый к клиенту на конечной точке, а также выгружается в отдельный файл по следующему пути:

  ```
  C:\ProgramData\SoftControl\Client.pem
  ```

- **Индивидуальный клиентский** – сертификат клиентской стороны, выдаваемый серверным компонентом после подтверждения регистрации[43] администратором через консоль управления SoftControl Admin Console. Данный сертификат уникален для каждого клиента, что делает невозможным несанкционированный доступ к каналу связи при наличии у злоумышленников украденного индивидуального сертификата другого клиента или общего сертификата. В случае если доверие к индивидуальному сертификату по какой-либо причине утеряно или истёк срок его действия, существует возможность выдачи другого сертификата (обновление[44]) или его отзыв (отклонение регистрации[43]).

7.2 Восстановление связи с сервером

В системе взаимодействия «клиент-сервер» (в рамках СИБ на основе Сервисного Центра) существует вероятность возникновения ситуаций, при которых IP-адрес сервера может быть изменён автоматически, например, при входе в сеть после перезагрузки. В этом случае клиентские приложения, в конфигурации которых прописаны только IP-адреса компьютера с установленным серверным компонентом SoftControl Server, а не его сетевое имя, теряют связь с ним. Чтобы не корректировать IP-адреса вручную локально в настройках каждого клиентского компонента, предусмотрен функционал резервного сервера восстановления. Для его активации выполните следующие шаги:

1) Откройте файл конфигурации сервера, расположенный по следующему пути:
   `C:\ProgramData\SoftControl\Server.Config.xml`
2) В элементе *RescueSettings* замените значение флага *Active* на *True*.
3) Добавьте в элемент *RescueSettings* подэлементы следующего вида:
   ```
   <Address Uri="<новый IP-адрес или NetBIOS-имя сервера>" Port="<порт связи>" />
   ```
4) Сохраните изменения в файле конфигурации.
5) Измените NetBIOS-имя компьютера с установленным SoftControl Server на *screstore*.
6) Перезагрузите компьютер с установленным SoftControl Server для применения новых настроек и изменения сетевого имени хоста.
7) После запуска системной службы SoftControl Server порт *8888* для резервного подключения будет автоматически добавлен в брандмауэр Windows.
8) По истечении 10 неудачных попыток подключения по списку адресов, заданных в настройках, клиентские компоненты будут предпринимать попытку подключения к резервному серверу с именем *screstore* на порт *8888* (по умолчанию). После успешного подключения по данному адресу, клиентам будет передан заданный в настройках новый список адресов сервера и произведена автоматическая замена старого списка адресов на обновленный в настройках. После того как соединение со всеми подключенными к Сервисному Центру клиентами будет восстановлено, сетевое имя сервера может быть изменено на изначальное.

7.3 Резервное копирование SoftControl Service Center

В некоторых случаях существует необходимость в создании резервной копии[149] компонентов Сервисного Центра, с целью дальнейшего восстановления[150] полностью работоспособной конфигурации без потери связи с клиентскими приложениями на удалённых хостах. Случаи, к которым применимы данные операции:

- необходимость переустановки ОС на компьютере с компонентами SoftControl Service Center;
- необходимость переноса SoftControl Service Center на другой компьютер.

7.3.1 Создание резервной копии

Резервная копия файлов SoftControl Service Center включает в себя необходимые для восстановления файлы конфигурации серверного компонента SoftControl Server и сертификаты[147]. Также могут быть сохранены пользовательские фильтры[120] SoftControl Admin Console (опционально). Чтобы создать резервную копию, выполните следующую последовательность действий:

1) В основном меню SoftControl Admin Console выберите пункт **Вид** → **Резервное копирование**.
2) В появившемся окне установите **Режим копирования** в области **Файлы сервера** (рис. Создание резервной копии[149]).

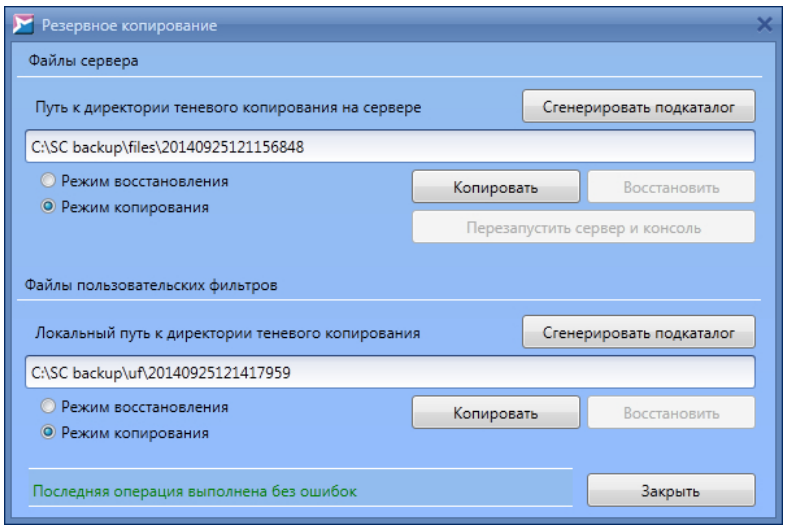


Рисунок 134. Создание резервной копии

Введите путь до каталога, куда предполагается сохранить файлы резервной копии, в соответствующее поле. Если требуется сформировать подкаталог с уникальным

идентификатором по введённому пути, нажмите на кнопку **Сгенерировать подкаталог**. Если нажать на указанную кнопку при пустом поле ввода, подкаталог будет по умолчанию располагаться в следующей директории:

```
C:\Windows\System32
```

Нажмите на кнопку **Копировать**, чтобы создать резервную копию файлов по выбранному пути. В нижней части окна будет отображён статус операции.

3) Для сохранения пользовательских фильтров в окне **Резервное копирование** (рис. Создание резервной копии 149) повторите действия п. 2 для области **Файлы пользовательских фильтров**.

   Если нажать на кнопку **Сгенерировать подкаталог** при пустом поле ввода, подкаталог будет по умолчанию располагаться в директории установки SoftControl Admin Console.

4) В случае, если БД Сервисного Центра располагается на внешнем сервере (отличном от компьютера с установленными компонентами SoftControl Service Center), сохранять её копию не требуется. В обратном случае создайте резервную текущей БД средствами Microsoft® SQL Server®.

7.3.2 Восстановление из резервной копии

Для восстановления SoftControl Service Center из резервной копии выполните следующую последовательность действий:

1) Убедитесь, что на компьютере установлено правильное время.
2) Установите 9 SoftControl Service Center той же версии, что использовался на компьютере, с которого создавалась резервная копия.
3) Выполните восстановление ранее сохранённой БД. Пропустите этот шаг, если БД находилась на другом компьютере и не удалялась.
4) Произведите первичную настройку сервера 19. При настройке укажите новое **Имя базы данных**, отличное от имени старой БД, чтобы не повредить данные в ней. После восстановления из резервной копии сервер автоматически переключится на старую базу данных.
5) В основном меню SoftControl Admin Console выберите пункт **Вид** → **Резервное копирование**.
6) В появившемся окне установите **Режим восстановления** в области **Файлы**

сервера (рис. Восстановление из резервной копии[151]). Введите путь до каталога с ранее сохранёнными файлами резервной копии в соответствующее поле и нажмите на кнопку **Восстановить**. В нижней части окна будет отображён статус операции.

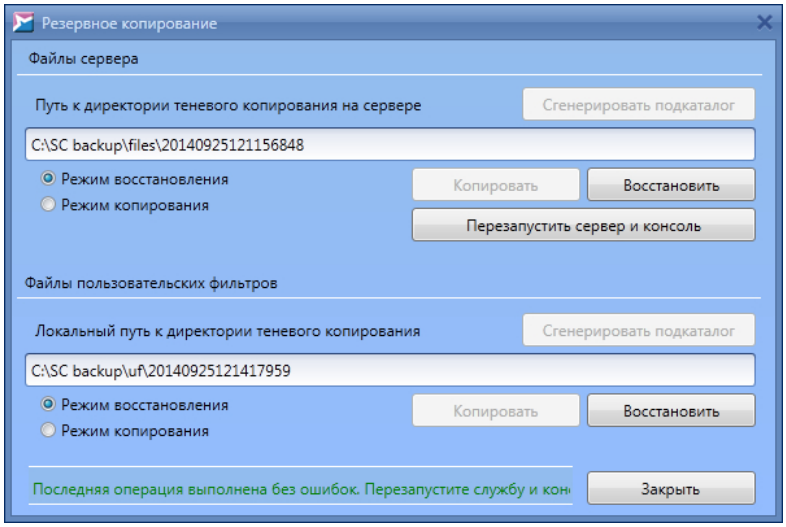


Рисунок 135. Восстановление из резервной копии

7) При необходимости восстановления пользовательских фильтров в окне **Резервное копирование** (рис. Восстановление из резервной копии[151]) повторите действия п. 6[150] для области **Файлы пользовательских фильтров**.
8) Нажмите на кнопку **Перезапустить сервер и консоль** для перезапуска системной службы SoftControl Server и применения восстановленной конфигурации.
   Примечание: на некоторых системах может также понадобиться перезагрузка компьютера.
9) Удалите временную базу данных, созданную на шаге 4[150].
10) Авторизуйтесь[24] в консоли управления SoftControl Admin Console. Проверьте работоспособность компонентов.

7.4 Источники

Источники дополнительной информации приведены в табл. 31.

Таблица 31. Вспомогательная документация

Название	Описание
Руководство пользователя SoftControl ATM Client	Руководство по установке, настройке и работе с клиентским компонентом SoftControl ATM Client.
Руководство пользователя SoftControl Endpoint Client	Руководство по установке, настройке и работе с клиентским компонентом SoftControl Endpoint Client.
Руководство пользователя SoftControl SClient	Руководство по установке, настройке и работе с клиентским компонентом SoftControl SClient.

Название	Описание
Руководство по установке SoftControl DLP Client	Руководство по установке и настройке клиентского компонента SoftControl DLP Client.

8. Диагностика проблем

В случае возникновения проблем при развёртывании и функционировании SoftControl Service Center, в первую очередь обратитесь к отчёту **SafenSoft** в журнале событий Windows. Для этого откройте Панель управления Windows, выберите раздел **Система и безопасность** (System and Security) → **Администрирование** (Administrative Tools), в нём откройте средство **Просмотр событий** (Event Viewer). В открывшемся окне в панели слева разверните категорию **Журналы приложений и служб** (Applications and Services Logs) и в ней выберите журнал **SafenSoft**. При анализе ошибок, предупреждений и уведомлений в данном отчёте может быть найдена причина, вызвавшая сбой при установке, запуске и установлении соединения между компонентами. Если определить причину самостоятельно невозможно, приложите файлы текстовых отчётов компонентов к запросу в техническую поддержку SAFE 'N SEC Corporation[154]. Список необходимых файлов приведен в табл. 32.

Таблица 32. Текстовые отчёты компонентов SoftControl Service Center

Вид отчёта компонента	Путь к файлу отчёта
Отчёт по работе консоли управления SoftControl Admin Console	`<каталог установки SoftControl Admin Console>\logs\ConsoleDetailedLog.txt`
Отчёт по работе серверного компонента SoftControl Server	`<каталог установки SoftControl Server>\logs\ServerDetailedLog.txt`

Системный отчёт клиентского компонента SoftControl SysWatch	ОС Microsoft® Windows® XP, Microsoft® Windows® Server 2003:
	`C:\Documents and Settings\All Users\Application Data\S.N.Safe&Software\Safe'n'Sec\Reports\system_<дд.мм.гг>_<чч.мм.сс.ммм>.txt`
	ОС Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012:
	`C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\system_<дд.мм.гг>_<чч.мм.сс.ммм>.txt`

9. Техническая поддержка

При возникновении вопросов по установке, настройке и работе SoftControl Service Center Вы можете обращаться в техническую поддержку по электронной почте support@safensoft.com.

10. Приложение

10.1 Установка и настройка Microsoft® SQL Server® 2008

Ниже приведена инструкция по установке и настройке СУБД Microsoft® SQL Server® 2008 для её совместного применения с программным продуктом SoftControl Service Center.

Подготовка к установке Microsoft® SQL Server® 2008

Перед установкой убедитесь, что система удовлетворяет минимальным требованиям к оборудованию и ПО для установки и запуска Microsoft® SQL Server® 2008 и, в случае наличия несоответствий заявленным требованиям, устраните их до начала установки.

Установка Microsoft® SQL Server® 2008

1) Запустите установочный файл Microsoft® SQL Server® 2008.
2) В окне Центра установки SQL Server (**SQL Server Installation Server**) откройте раздел **Installation** и выберите тип установки **New SQL Server stand-alone installation or add features to an existing installation** (рис. Раздел "Installation" 155).

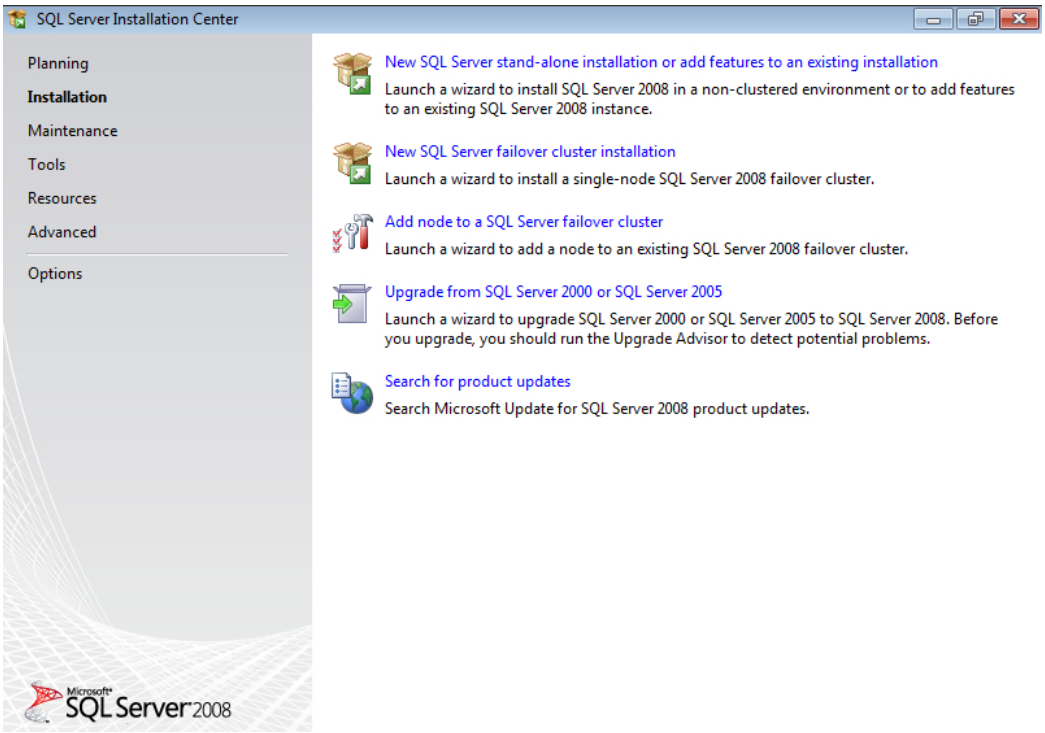


Рисунок 136. Раздел "Installation"

3) В разделе **Setup Support Rules** выполняется проверка на возможные проблемы, которые могут возникнуть при установке вспомогательных файлов установки Microsoft® SQL Server® 2008 (рис. Проверка проблем при установке вспомогательных файлов 156). Ошибки должны быть исправлены перед продолжением установки. Если проблем нет, то нажмите на кнопку **OK**.

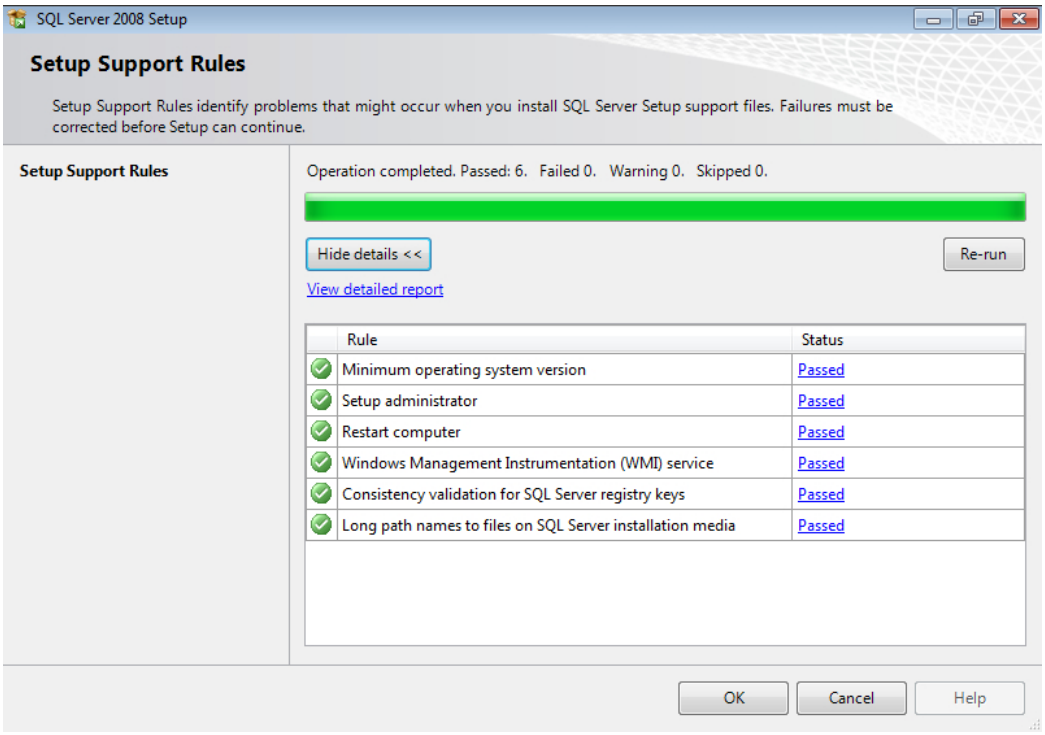


Рисунок 137. Проверка проблем при установке вспомогательных файлов

4) В разделе **Product Key** выберите вариант **Enter the product key**, введите лицензионный ключ для Microsoft® SQL Server® 2008 и нажмите на кнопку **Next** (рис. Раздел "Product Key" 156).

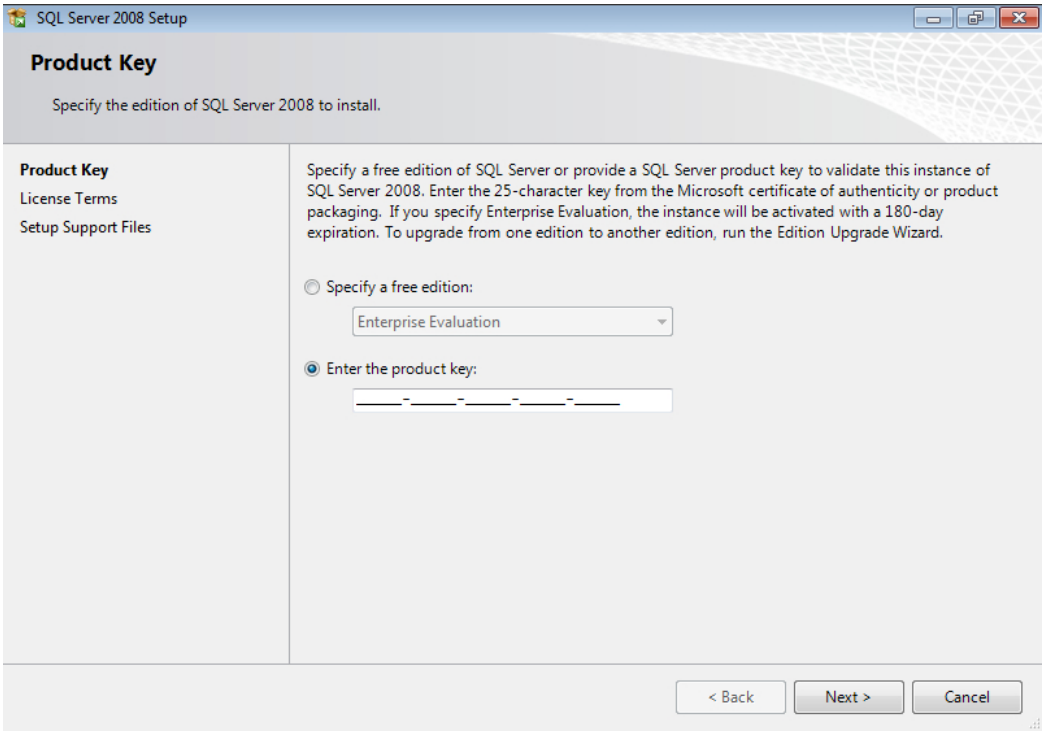


Рисунок 138. Раздел "Product Key"

5) Прочитайте условия лицензионного соглашения (**License Terms**) и, если Вы с ними согласны, то установите флажок **I accept the license terms** и нажмите на кнопку **Next** (рис. Раздел "License Terms" 157).

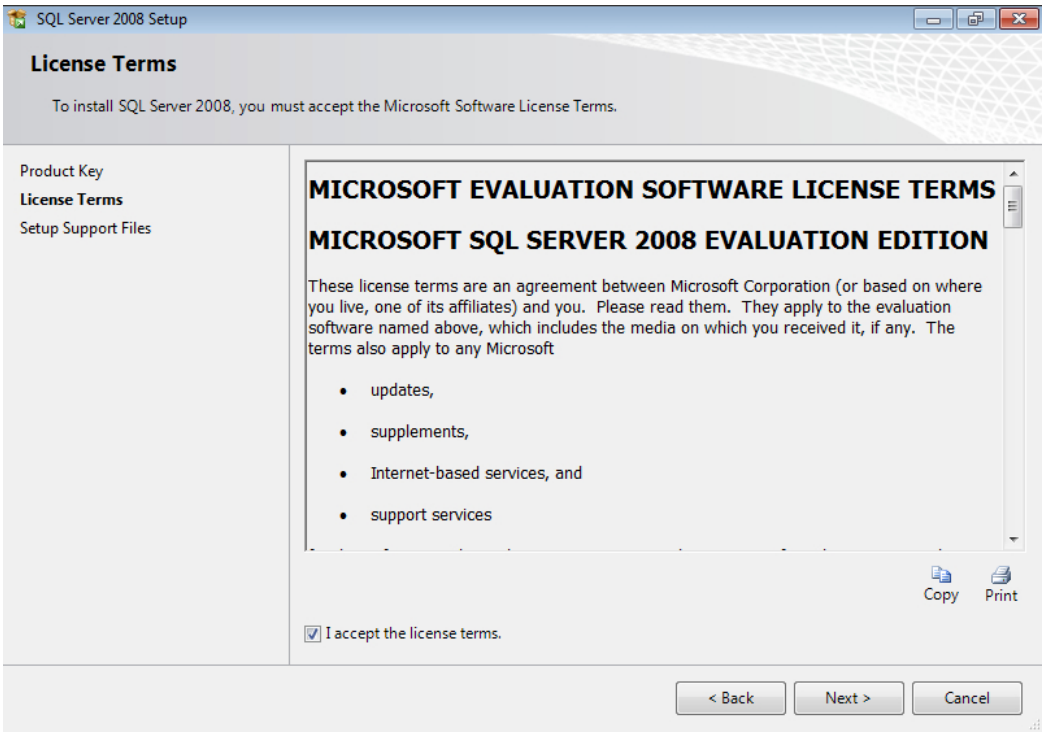


Рисунок 139. Раздел "License Terms"

6) В разделе **Setup Support Files** нажмите на кнопку **Install** (рис. Раздел "Setup Support Files" 158).

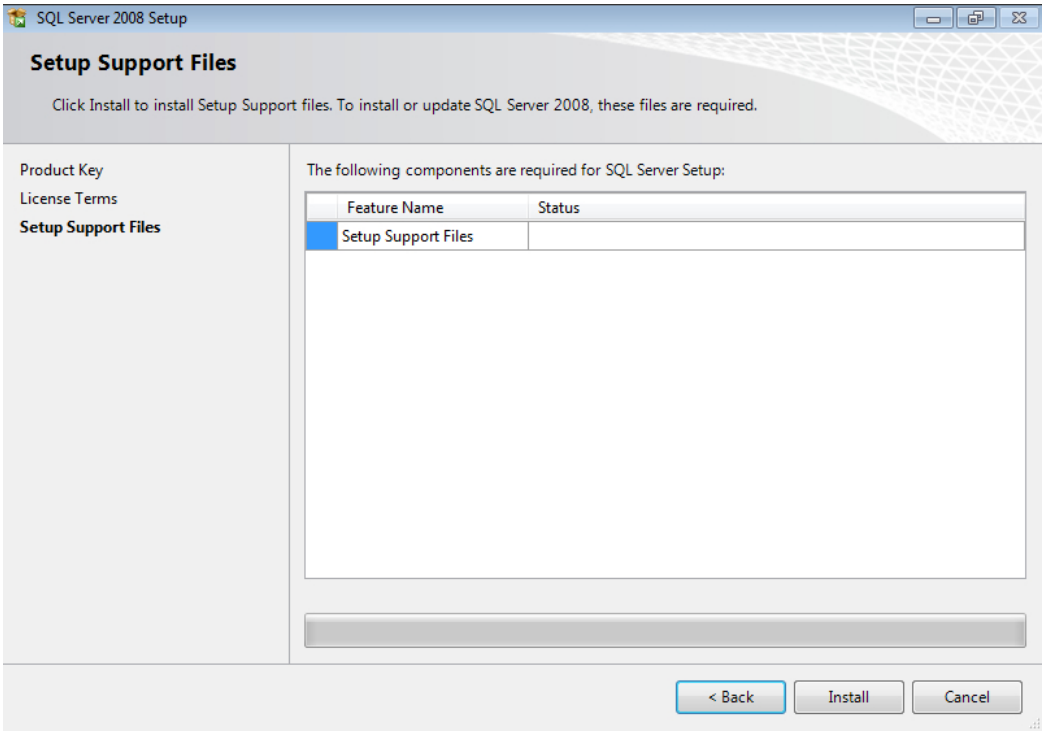


Рисунок 140. Раздел "Setup Support Files"

7) В разделе **Setup Support Rules** выполняется проверка на возможные проблемы, которые могут возникнуть при установке вспомогательных файлов установки Microsoft® SQL Server® 2008 (рис. Раздел "Setup Support Rules". Подробные данные 158). Ошибки должны быть исправлены перед продолжением установки. Если проблем нет, то нажмите на кнопку **Next**.

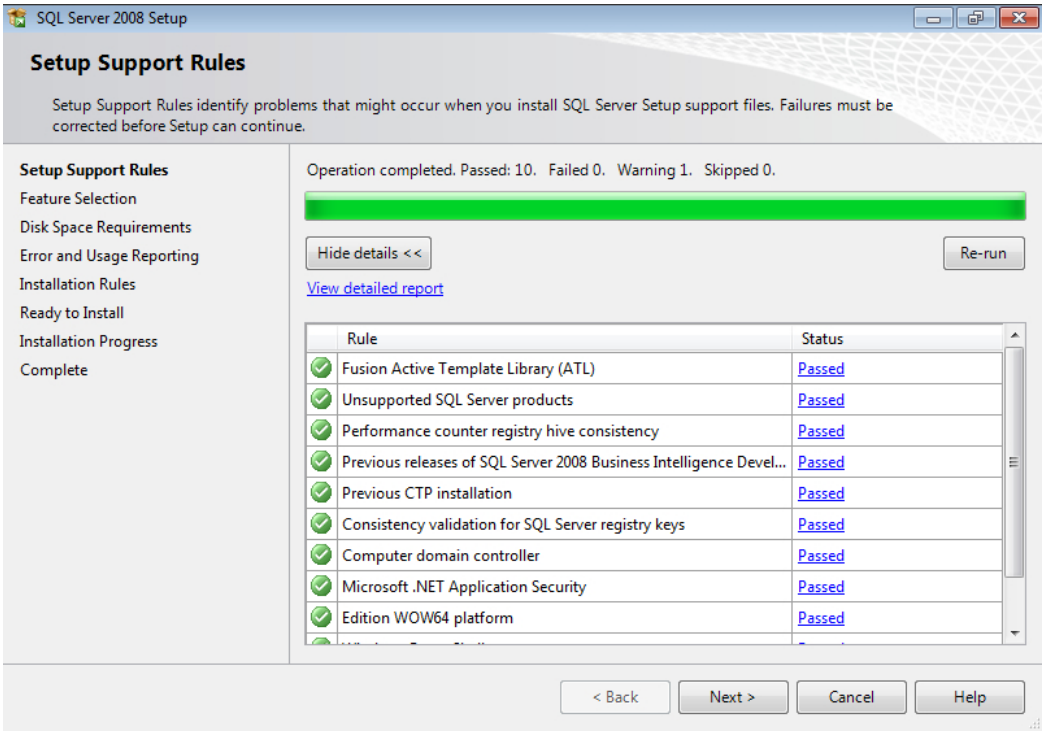


Рисунок 141. Раздел "Setup Support Rules". Подробные данные

8) В разделе **Feature Selection** нажмите на кнопку **Select All**, укажите путь для установки в поле **Shared feature directory** и нажмите на кнопку **Next** (рис. Раздел "Feature Selection" 159).

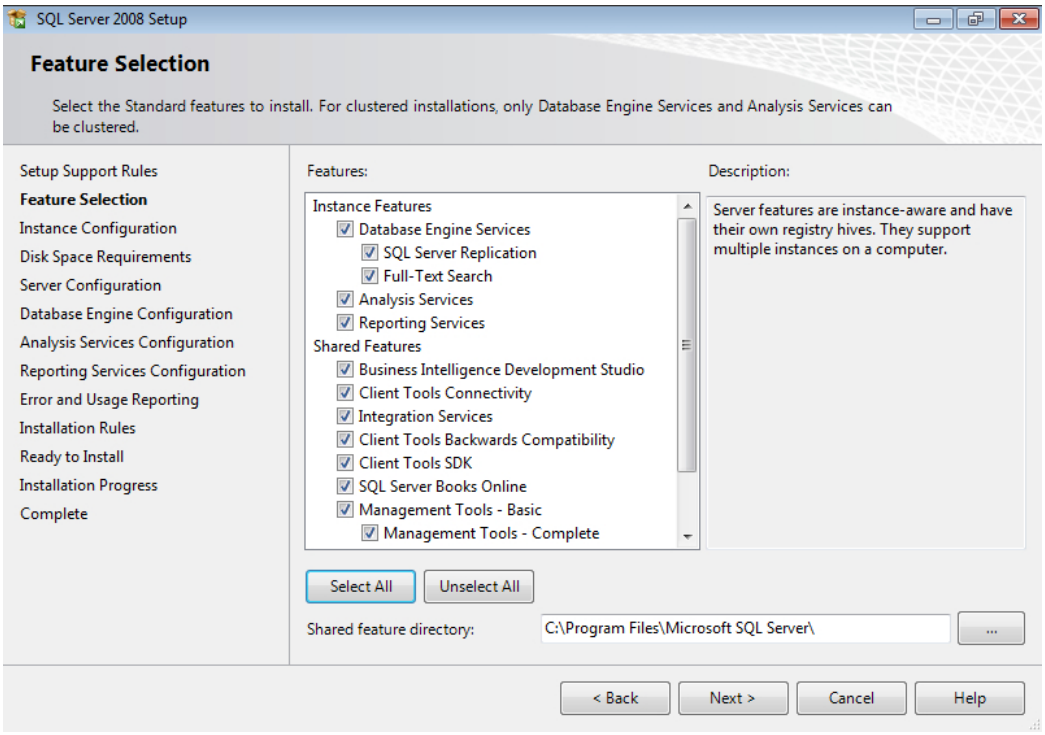


Рисунок 142. Раздел "Feature Selection"

9) В разделе **Instant Configuration** выберите параметр **Default Instance** и нажмите на кнопку **Next** (рис. Раздел "Instance Configuration" 160).

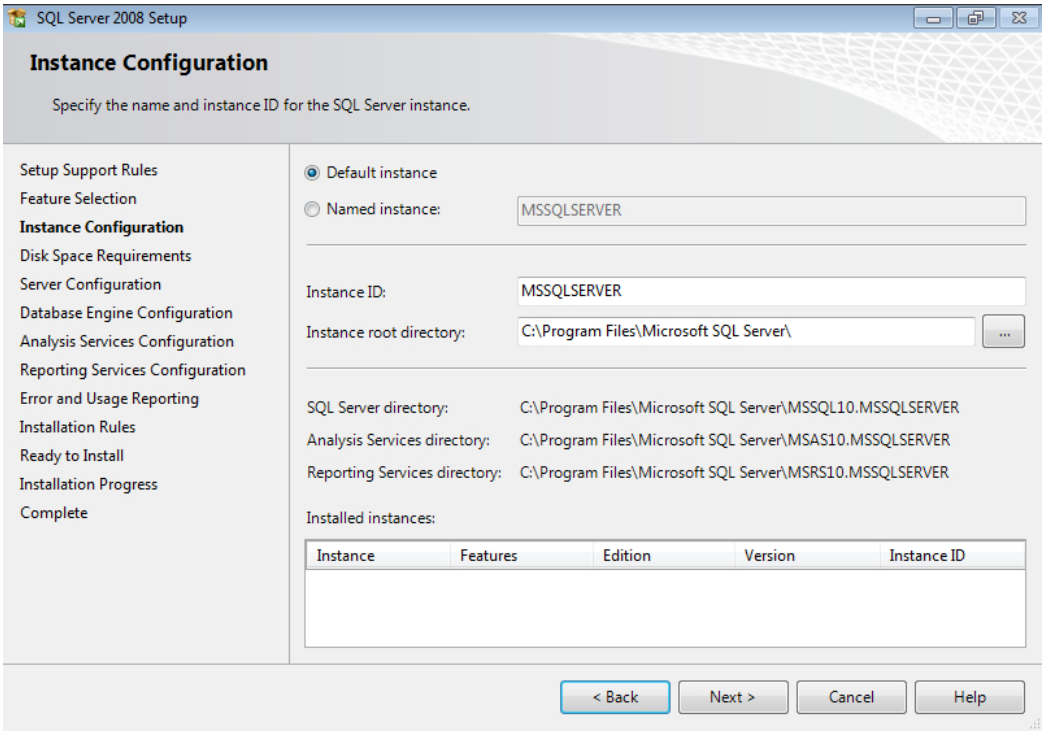


Рисунок 143. Раздел "Instance Configuration"

10) В разделе **Disc Space Requirements** нажмите на кнопку **Next** (рис. Раздел "Disc Space Requirements" 160).

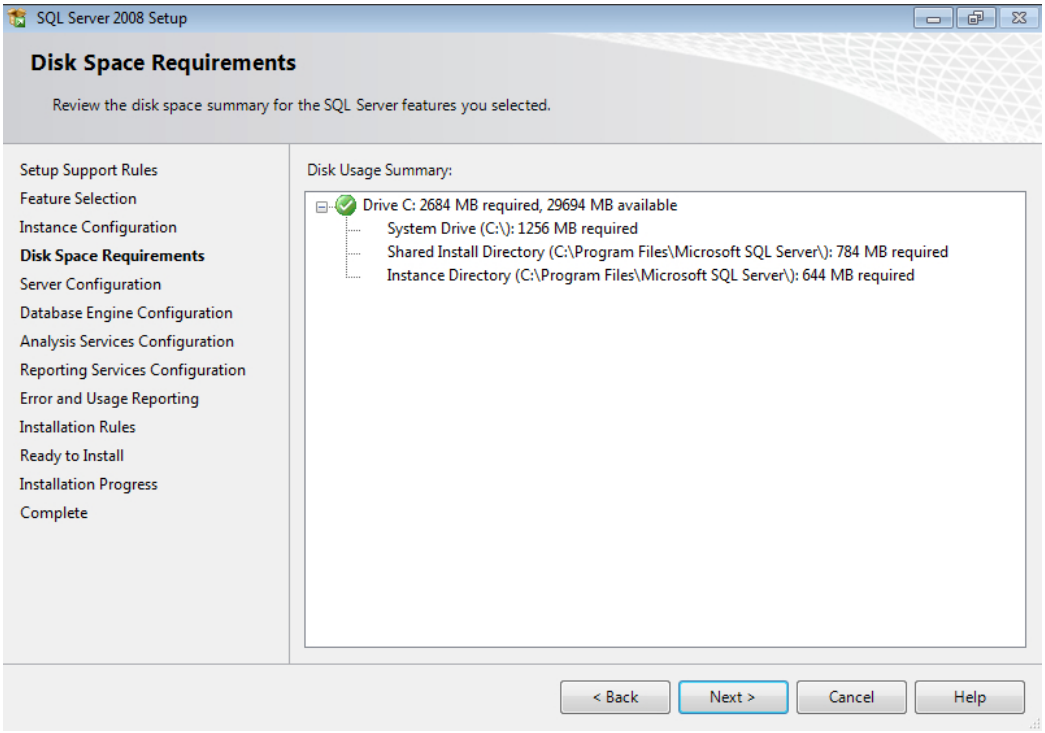


Рисунок 144. Раздел "Disc Space Requirements"

11) В разделе **Server Configuration** на вкладке **Service Accounts** нажмите на кнопку **Use the same account for all SQL Server services** (рис. Вкладка "Service Accounts" раздела "Server Configuration" 161).

В открывшемся окне выберите учетную запись **NETWORK SERVICE** и нажмите на кнопку **OK** (рис. Учётная запись 162).

На вкладке **Collation** для компонентов **Database Engine** и **Analysis Services** установите параметр **Cyrillic_General_CI_AS** (рис. Вкладка "Collation" раздела "Server Configuration" 162).

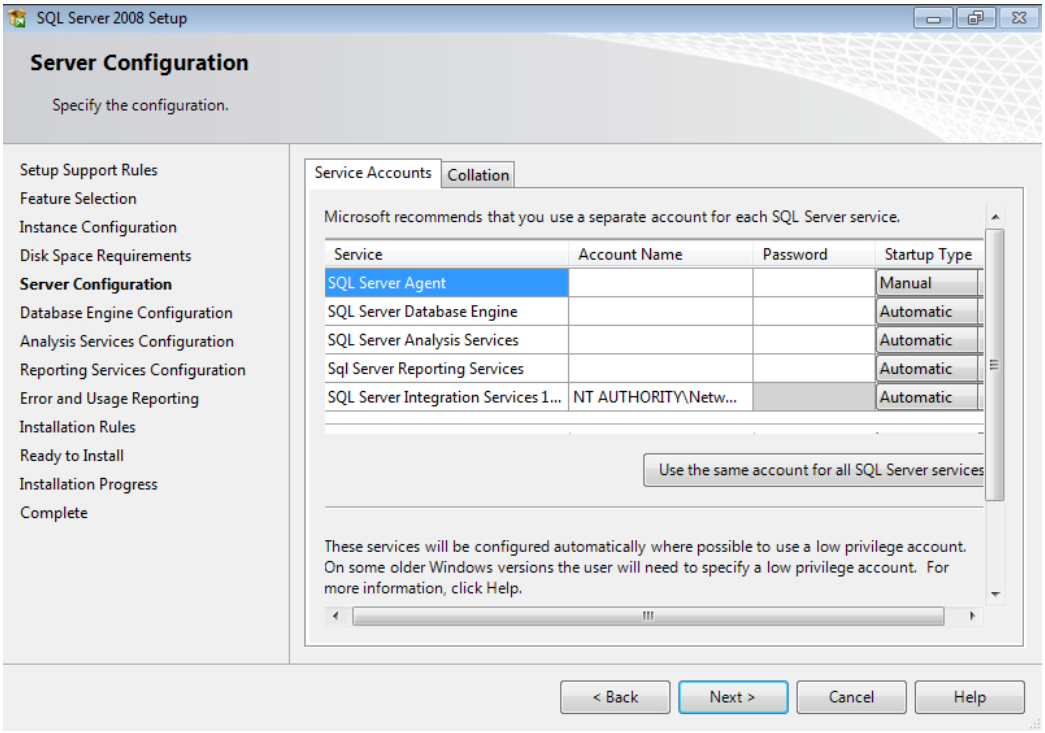


Рисунок 145. Вкладка "Service Accounts" раздела "Server Configuration"

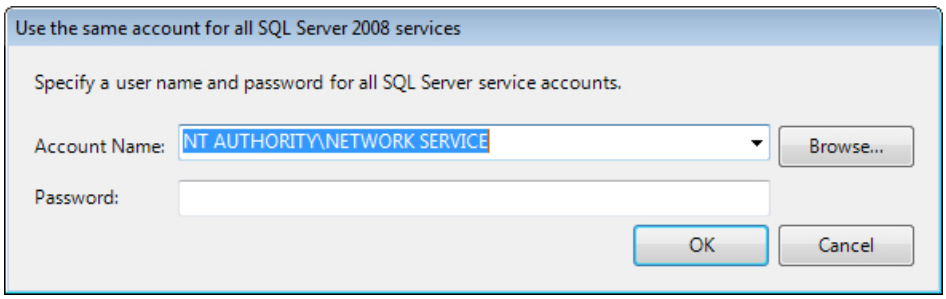


Рисунок 146. Учётная запись

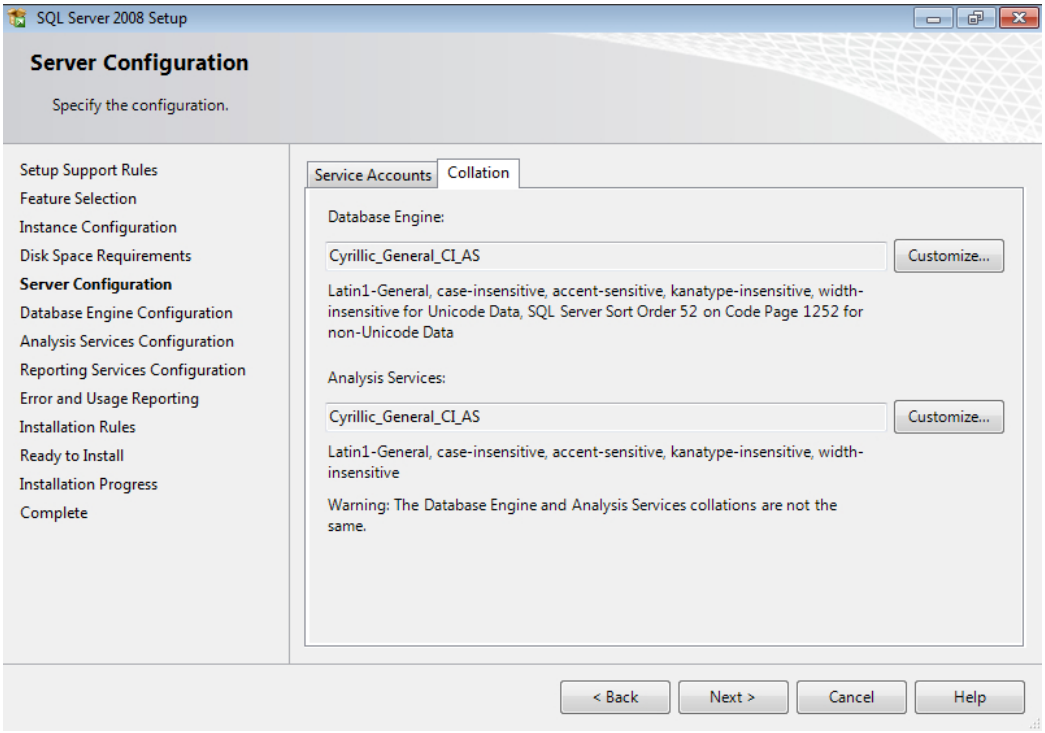


Рисунок 147. Вкладка "Collation" раздела "Server Configuration"

Для этого нажмите на кнопку **Customize** для компонента **Database Engine**, в открывшемся окне установите переключатель в положение **Windows collation designator and sort order**, в выпадающем списке **Collation designator** выберите параметр **Cyrillic_General**, установите флажок **Accent-sensitive** и нажмите на кнопку **OK** (рис. Установка параметров "Collation" для "Database Engine" 163).

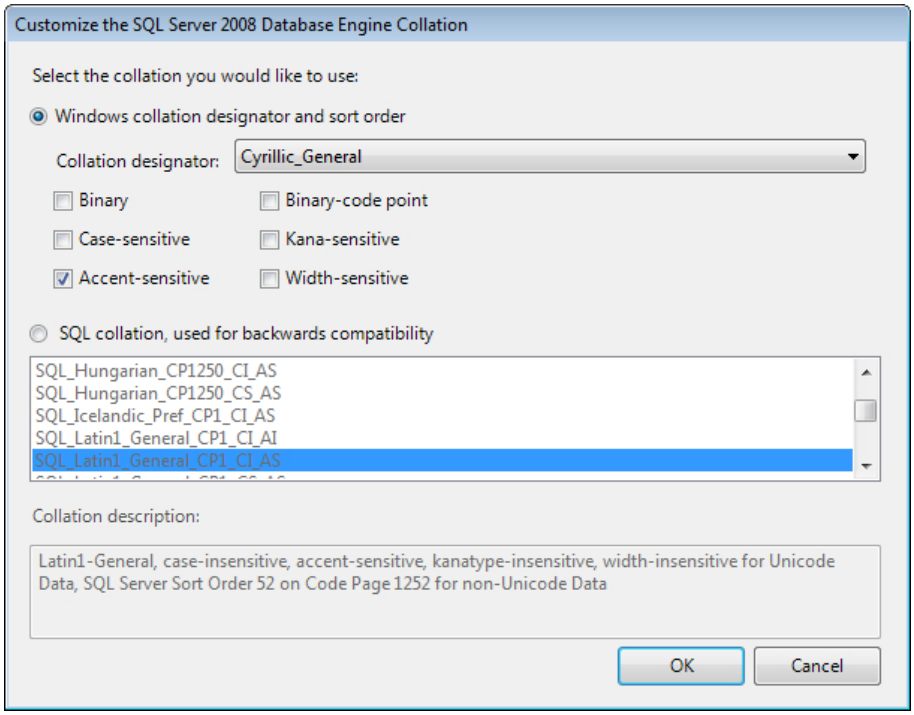


Рисунок 148. Установка параметров "Collation" для "Database Engine"

Нажмите на кнопку **Customize** для компонента **Analysis Services**, в открывшемся окне в выпадающем списке **Collation designator** выберите параметр **Cyrillic_General**, установите флажок **Accent-sensitive** и нажмите на кнопку **OK** (рис. Установка параметров "Collation" для "Analysis Services" 164).

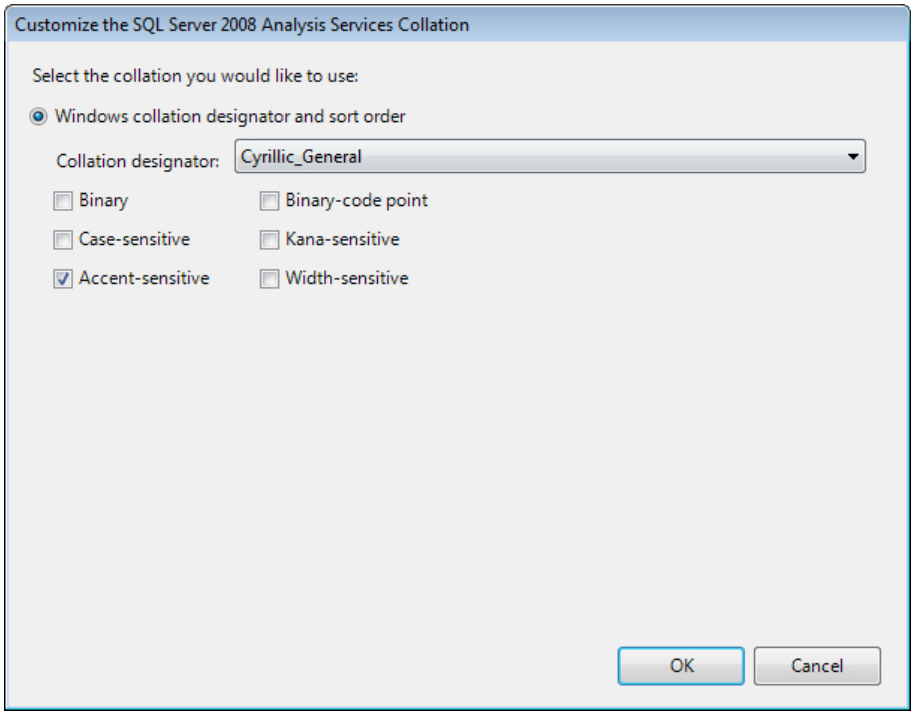


Рисунок 149. Установка параметров "Collation" для "Analysis Services"

В разделе **Server Configuration** нажмите на кнопку **Next** для продолжения установки.

12) В разделе **Database Engine Configuration** выберите параметр **Mixed Mode** и задайте пароль для учётной записи **Built-in SQL Server system administrator account** в поле **Enter password** и его подтверждение в поле **Confirm password** (рис. Раздел "Database Engine Configuration" 165). Нажмите на кнопку **Add Current User** и убедитесь, что в списке **Specify SQL Server administrators** отображается текущая системная учётная запись, после чего нажмите на кнопку **Next**.

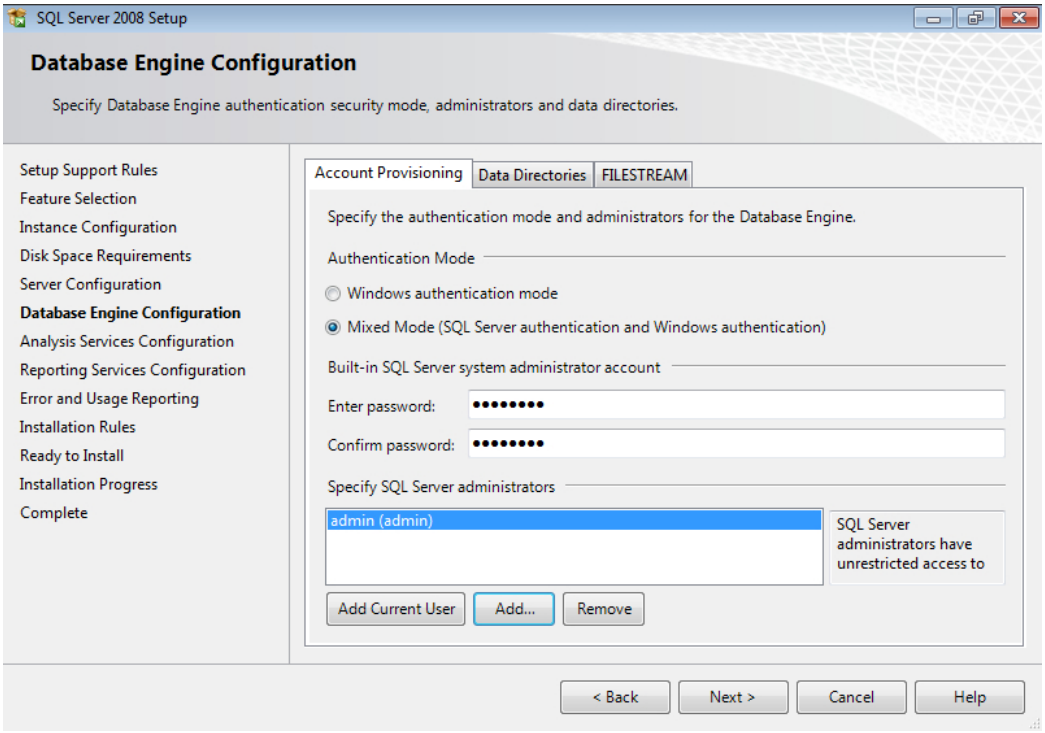


Рисунок 150. Раздел "Database Engine Configuration"

13) В разделе **Analysis Services Configuration** на вкладке **Account Provisioning** нажмите на кнопку **Add Current User** и убедитесь, что в списке **Specify which users have administrative permissions for Analysis Services** отображается текущая учётная запись, после чего нажмите на кнопку **Next** (рис. Раздел "Analysis Services Configuration" 166).

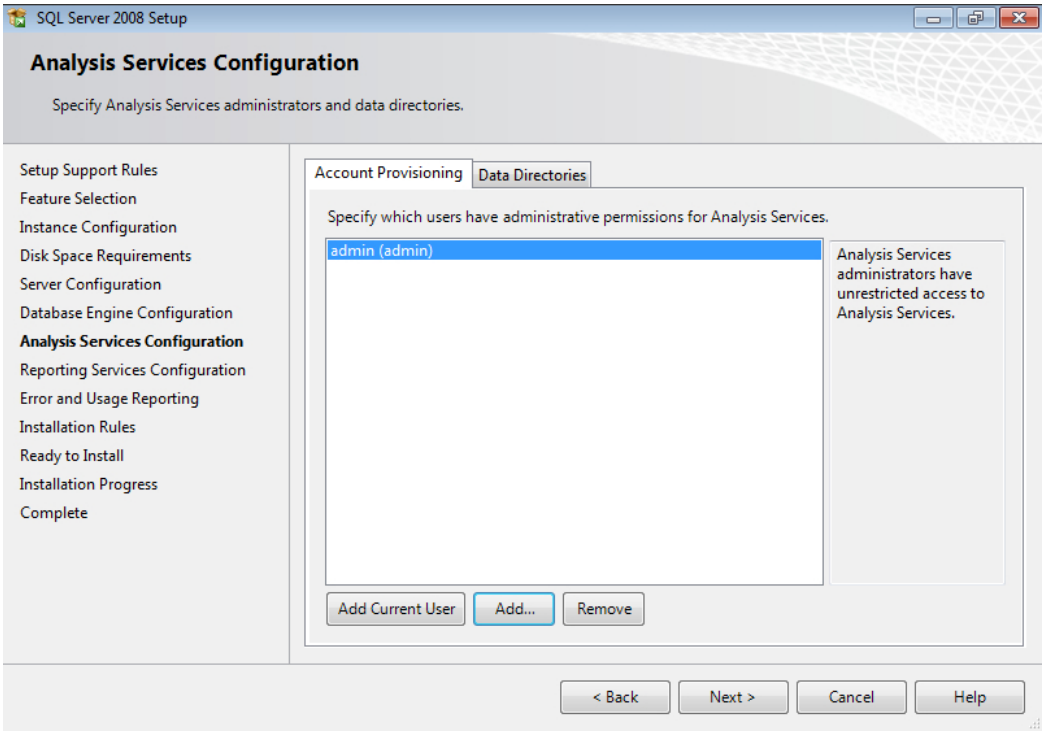


Рисунок 151. Раздел "Analysis Services Configuration"

14) В разделе **Reporting Services Configuration** выберите параметр **Install the native mode default configuration** и нажмите на кнопку **Next** (рис. Раздел "Reporting Services Configuration" 167).

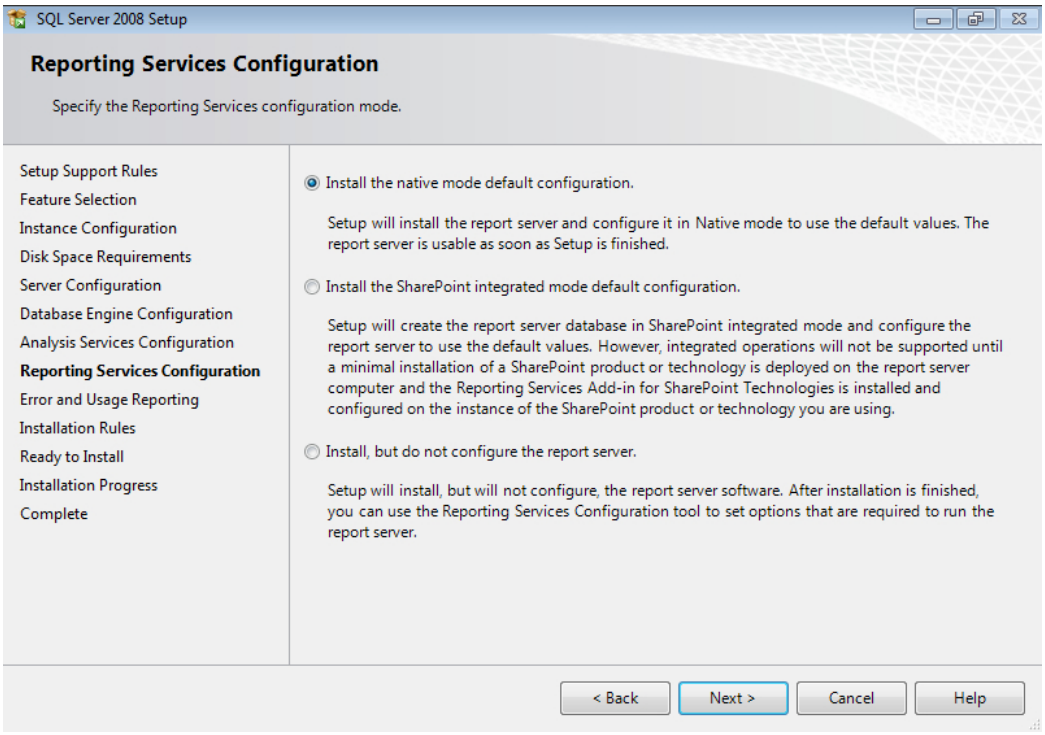


Рисунок 152. Раздел "Reporting Services Configuration"

15) В разделе **Error and Usage Reporting** нажмите на кнопку **Next** (рис. Раздел "Error and Usage Reporting" 168).

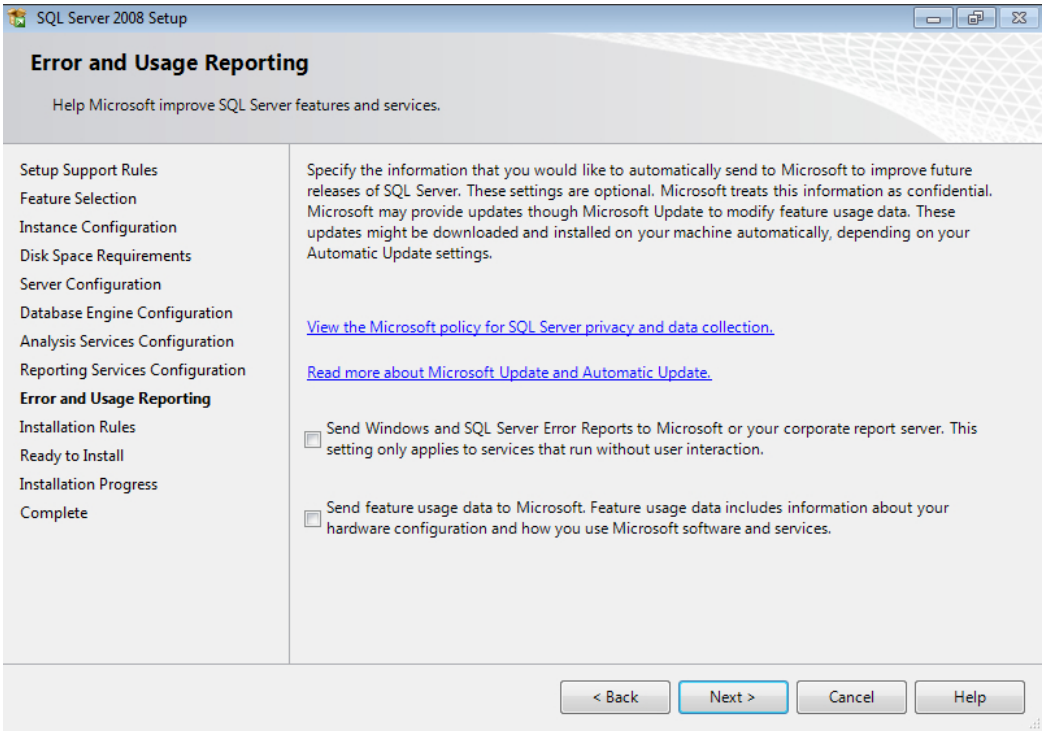


Рисунок 153. Раздел "Error and Usage Reporting"

16) В разделе **Installation Rules** выполняется проверка на возможные проблемы, которые могут возникнуть при установке Microsoft® SQL Server® 2008 (рис. Раздел "Installation Rules" 168). Если ошибок не найдено, то нажмите на кнопку **Next**.

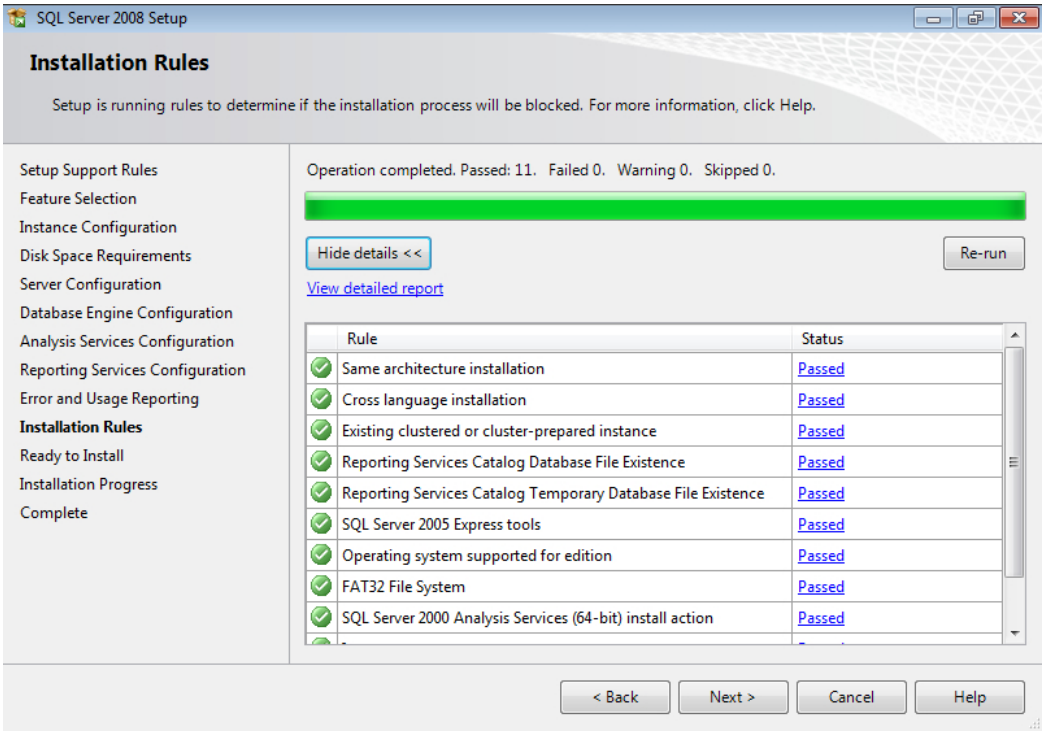


Рисунок 154. Раздел "Installation Rules"

17) В разделе **Ready to Install** проверьте состав устанавливаемых компонентов и нажмите на кнопку **Install** (рис. Раздел "Ready to Install" 169).

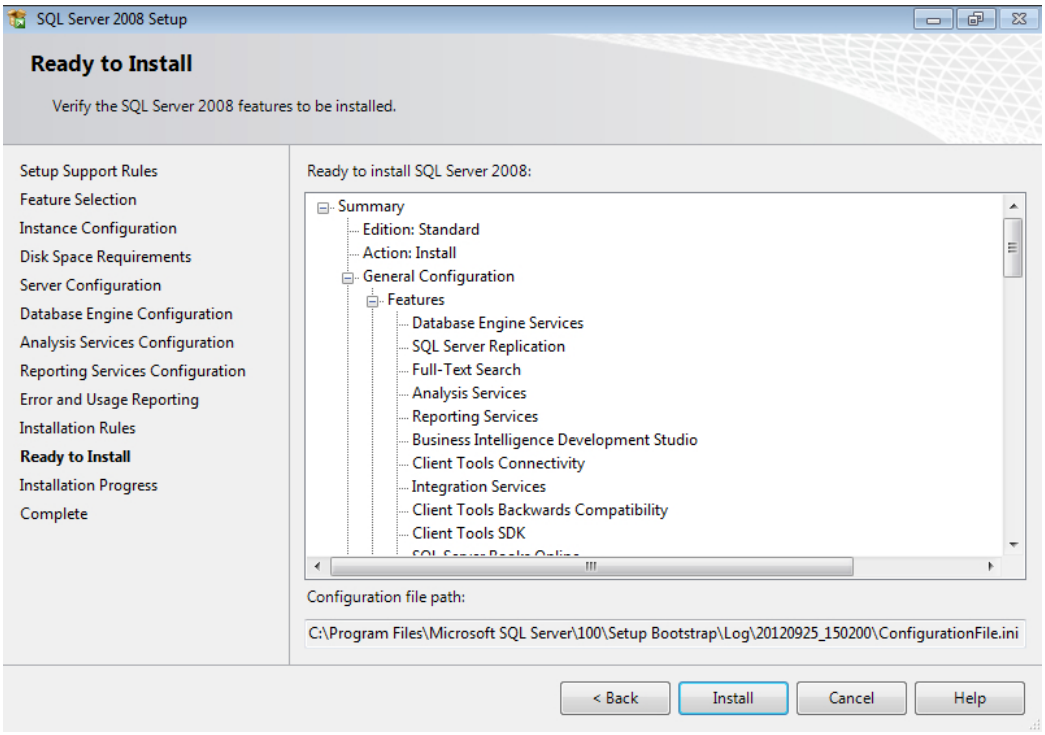


Рисунок 155. Раздел "Ready to Install"

18) В разделе **Installation Progress** отображается процесс установки компонентов Microsoft® SQL Server® 2008 (рис. Раздел "Installation Progress" 170).

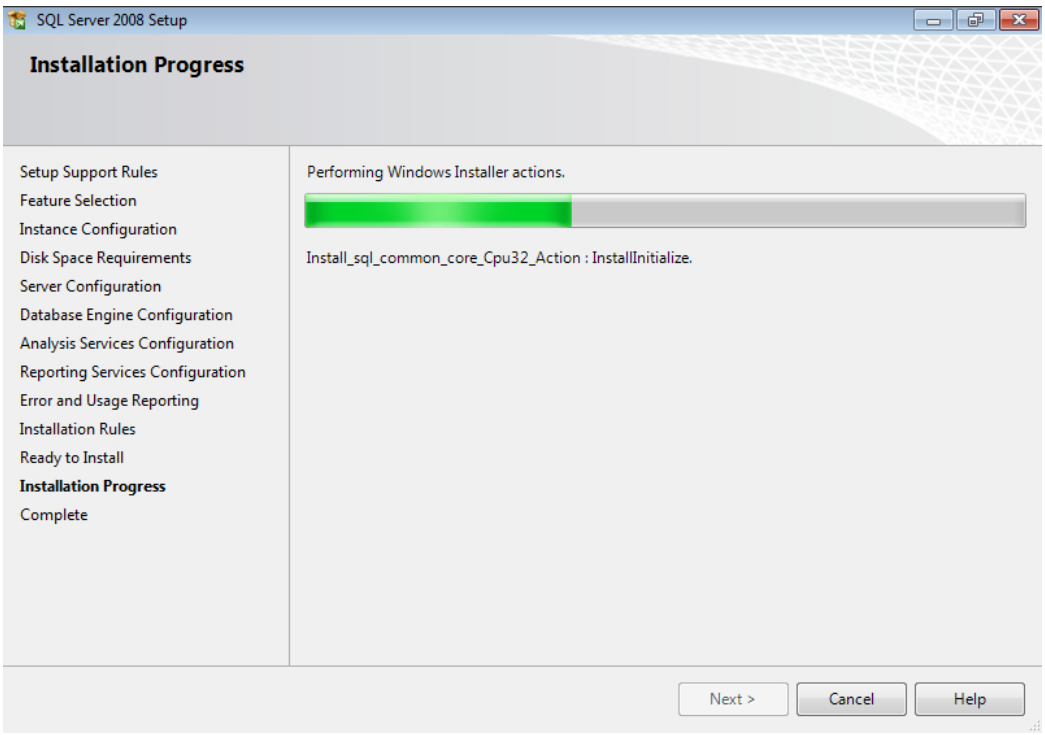


Рисунок 156. Раздел "Installation Progress"

После окончания установки нажмите на кнопку **Next**.

Для завершения установки в разделе **Complete** нажмите на кнопку **Close** (рис. Раздел "Complete" 170).

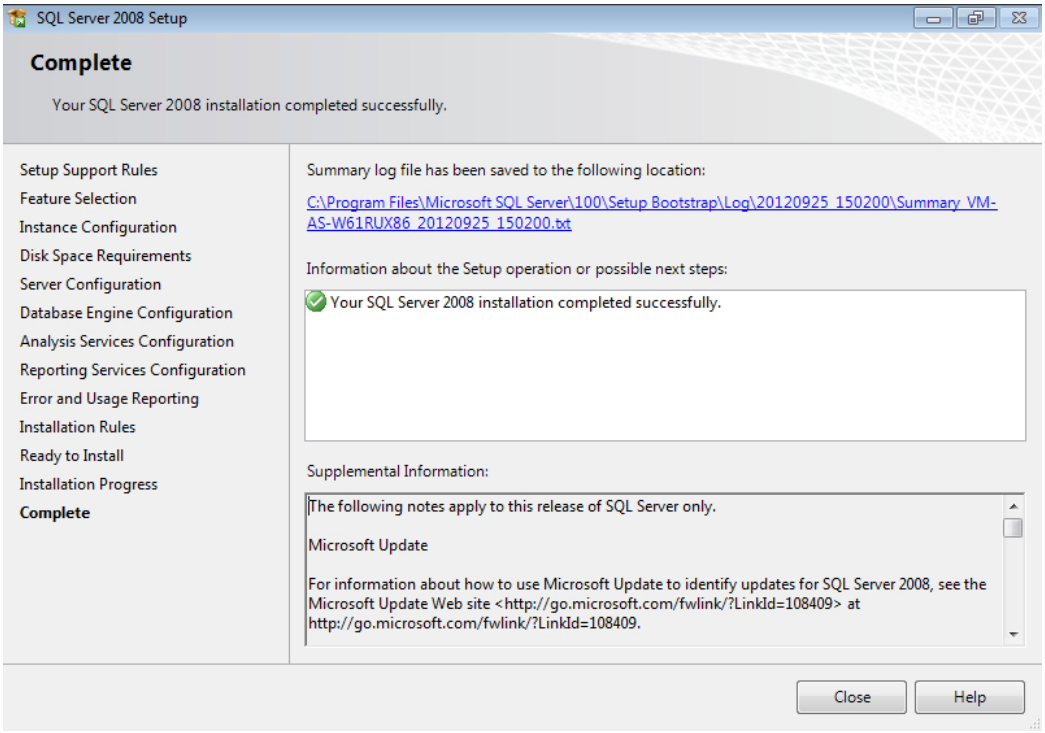


Рисунок 157. Раздел "Complete"

10.2 Добавление компонента Desktop Experience

Примечание: продемонстрировано на примере ОС Microsoft® Windows® Server 2008 R2.

1) Откройте оснастку **Server Manager** из раздела **Administrative Tools** меню **Start**. Перейдите в раздел **Features** и в области **Features Summary** нажмите на кнопку **Add Features** (рис. Оснастка Server Manager 171).

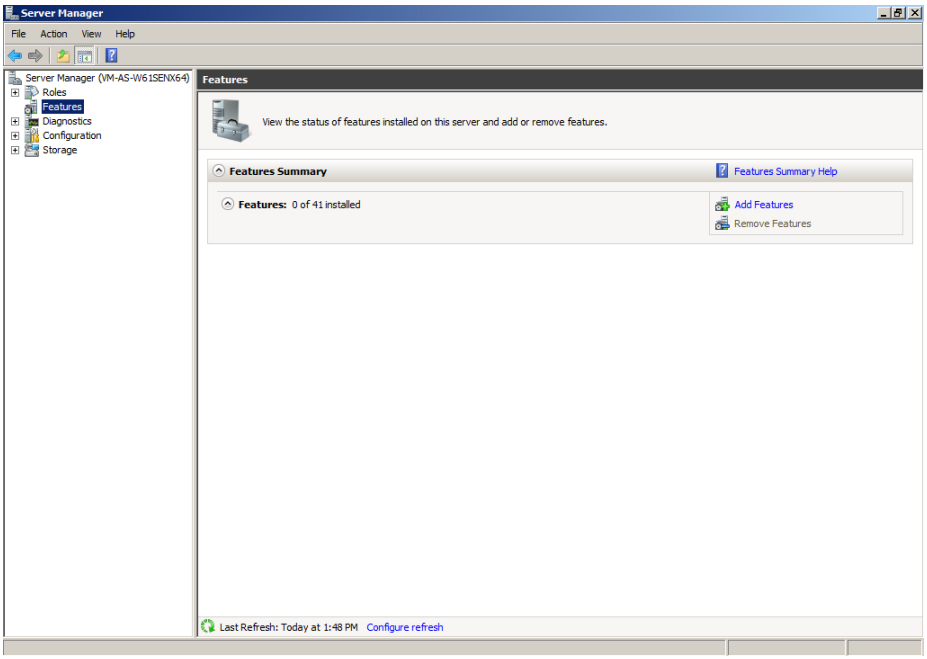


Рисунок 158. Оснастка Server Manager

2) В появившемся окне **Add Features Wizard** установите флажок у компонента **Desktop Experience** (рис. Выбор компонентов для добавления [172]) (в Microsoft® Windows® Server 2012/2012 R2: **User Interfaces and Infrastructure** → **Desktop Experience**).

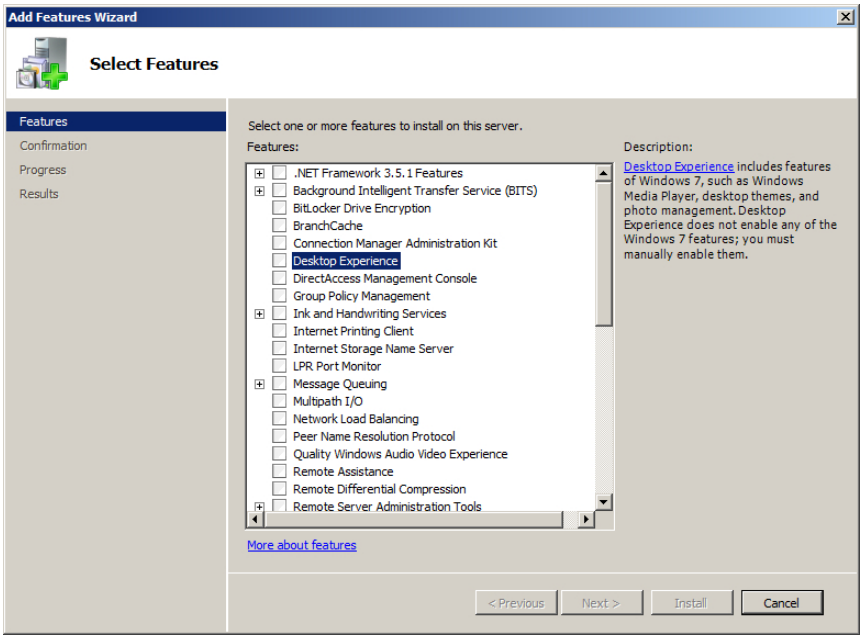


Рисунок 159. Выбор компонентов для добавления

3) При появлении диалогового окна с информацией о необходимости добавления связанных компонентов выберите вариант **Add Required Features** (рис. Запрос добавления связанных компонентов [172]).

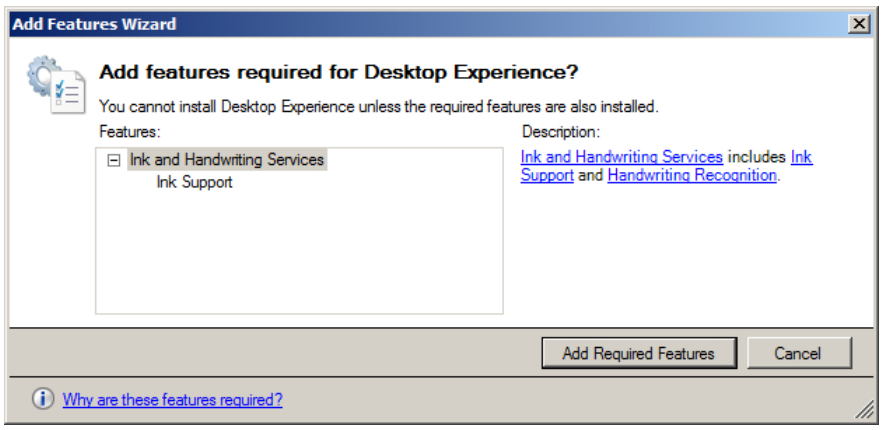


Рисунок 160. Запрос добавления связанных компонентов

4) Убедитесь, что компонент **Desktop Experience** выбран и нажмите на кнопку **Next** (рис. Выбор компонентов для добавления [172]).

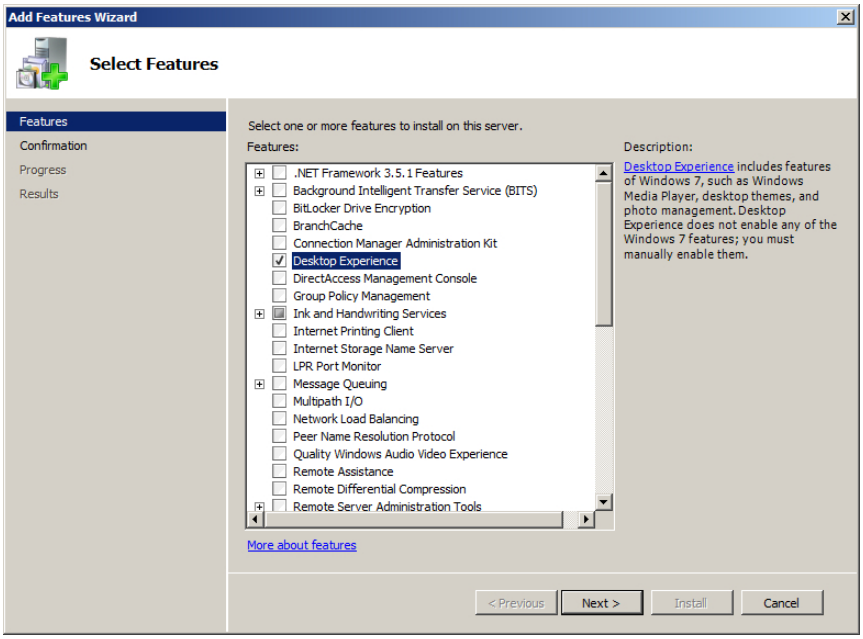


Рисунок 161. Выбор компонентов для добавления

5) На шаге **Confirmation** нажмите на кнопку **Next** (рис. Подтверждение добавления компонентов 173).

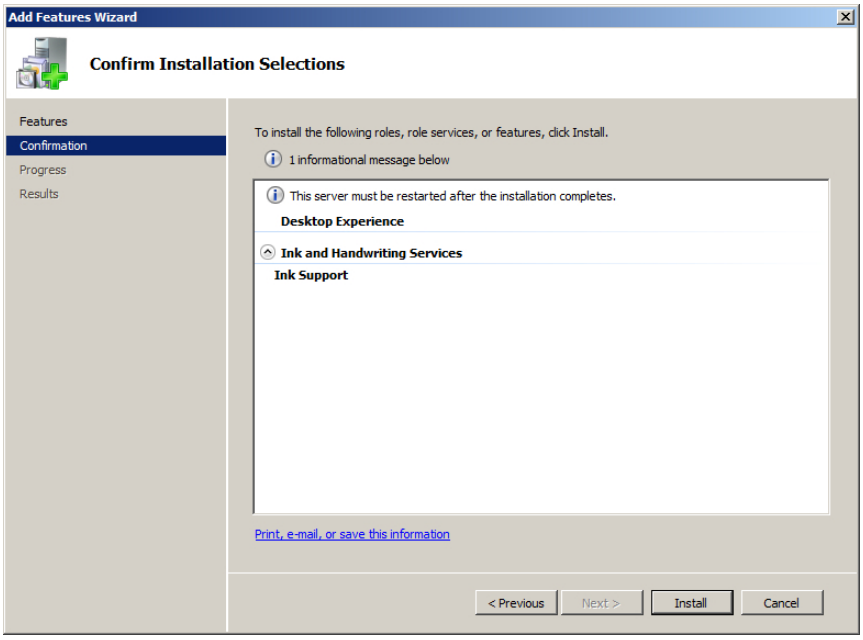


Рисунок 162. Подтверждение добавления компонентов

6) Дождитесь завершения установки (рис. Процесс установки 173).

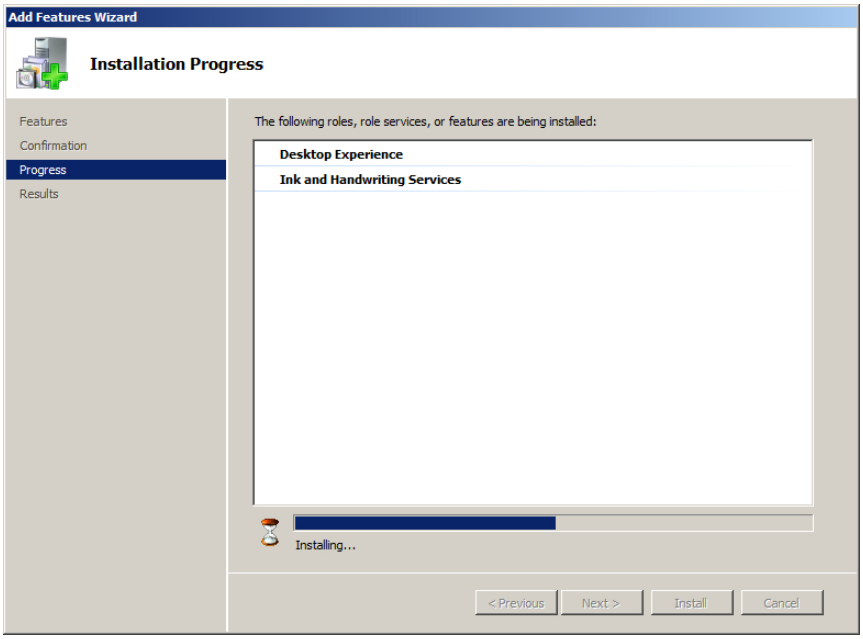


Рисунок 163. Процесс установки

7) На шаге **Results** нажмите на кнопку **Close** (рис. Завершение добавления компонентов 174).
8) В диалоговом окне с предложением перезапуска системы выберите **Yes**, после чего система будет отправлена на перезагрузку для завершения установки (рис. Запрос перезагрузки 174).
9) После перезапуска системы в появившемся окне **Resume Configuration Wizard** убедитесь, что все требуемые компоненты установлены успешно (**Installation succeeded**) и нажмите на кнопку **Close** (рис. Результат добавления компонентов 175).

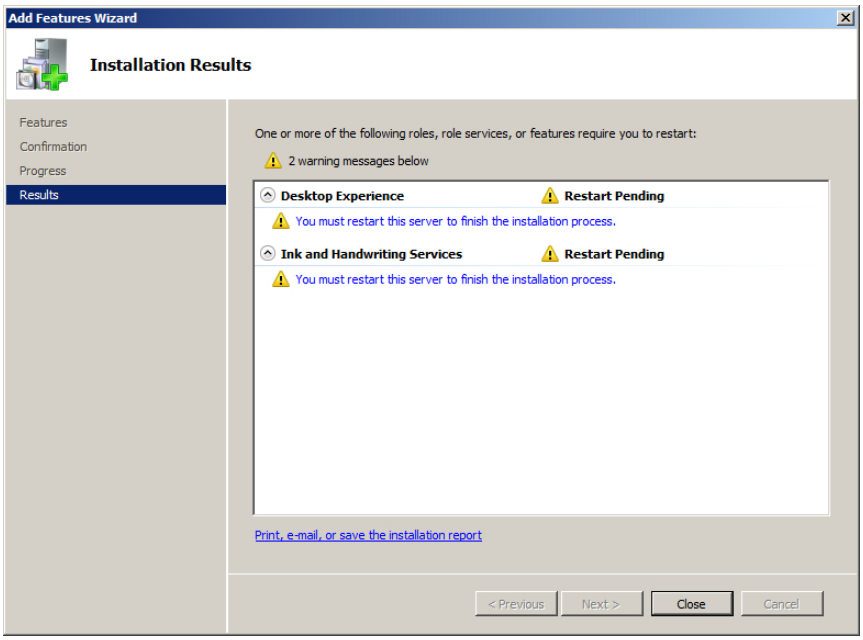


Рисунок 164. Завершение добавления компонентов

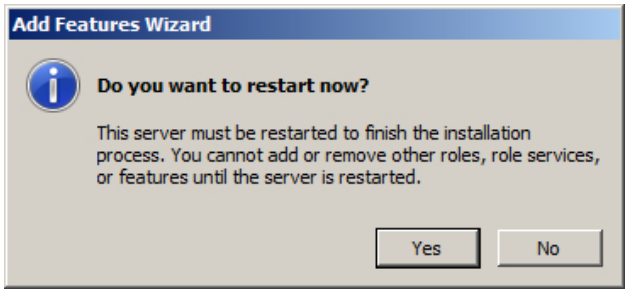


Рисунок 165. Запрос перезагрузки

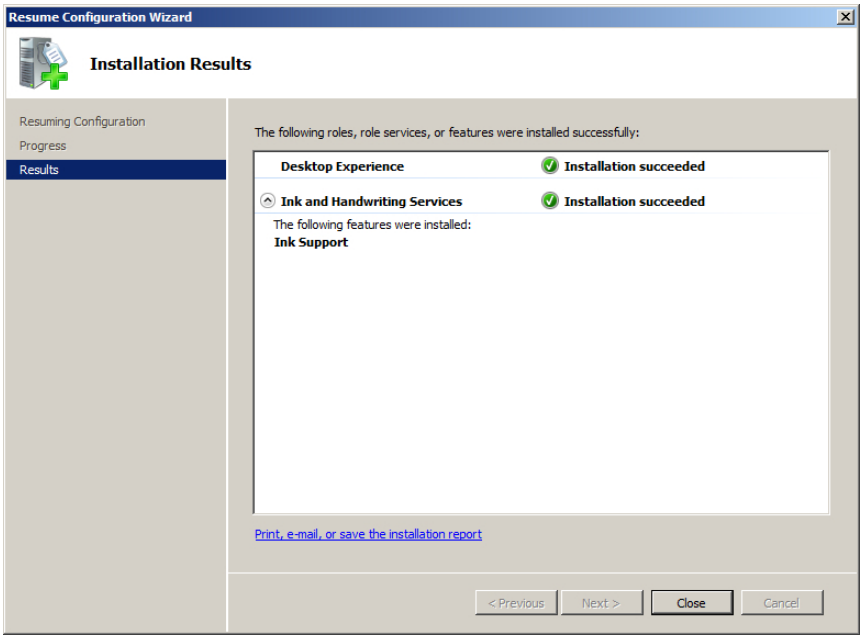


Рисунок 166. Результат добавления компонентов